

L'impatto delle tecnologie di sorveglianza biometrica sui diritti umani fondamentali: uno studio comparativo tra Cina e Canada

Antonella Benedetto*

THE IMPACT OF SURVEILLANCE BIOMETRIC TECHNOLOGIES ON FUNDAMENTAL HUMAN RIGHTS: A COMPARATIVE STUDY OF CHINA AND CANADA

ABSTRACT: The article examines the use of biometric surveillance as a concerning technology that affects several fundamental human rights in both China and Canada. Specifically, it explores the differing interpretations of human rights between the two countries through case studies, including Canada's border surveillance system and the securitisation of its borders. In the case of China, the article delves into human rights violations in Xinjiang and the extensive implementation of the Social Credit System (SCS).

KEYWORDS: international security; surveillance; artificial intelligence; human rights; privacy

ABSTRACT: L'articolo analizza l'uso della sorveglianza biometrica come una tecnologia preoccupante che influisce su diversi diritti umani fondamentali, con un focus specifico su Cina e Canada. In particolare, si esamina come i diritti umani siano considerati in modo differente tra i due Paesi, attraverso l'analisi di casi di studio: il sistema di sorveglianza delle frontiere e la securitarizzazione dei confini in Canada. Per quanto riguarda la Cina, l'attenzione si concentra sulle violazioni dei diritti umani nella regione dello Xinjiang e sull'implementazione su larga scala del Sistema di Credito Sociale (SCS).

PAROLE CHIAVE: sicurezza internazionale; sorveglianza; Intelligenza Artificiale; diritti umani; privacy

SOMMARIO: 1. Introduzione – 2. Cosa si intende per sorveglianza biometrica? – 3. La concezione dei diritti umani in Asia e in Occidente – 4. Breve storia della legislazione cinese sulla privacy – 4.1. Il Sistema di Credito Sociale (SCS): impatto sui diritti umani fondamentali – 4.2. La Regione Autonoma Uigura dello Xinjiang – 5. Il Canada e la sua legislazione sulla privacy – 5.1. La securitarizzazione delle frontiere in Canada – 5.2. Evoluzioni recenti tra immigra-

* Antonella Benedetto ha conseguito la Laurea Magistrale in International Security Studies presso l'Università di Trento e la Scuola Superiore Sant'Anna di Pisa. Attualmente lavora presso la Commissione Europea. Mail: antobenedetto@alice.it. Le opinioni espresse sono esclusivamente dell'autore, formulate a titolo personale, e non rappresentano la posizione della Commissione Europea. Contributo sottoposto a doppio referaggio anonimo.

zione e regolamentazione – 6. Unione Europea: *Artificial Intelligence Act (AI Act)* e il divieto di identificazione biometrica in tempo reale – 7. Osservazioni conclusive.

Nel 2023, 23

Il mio cuore batterà fra le stelle

Ma sarà una macchina che

Lo farà battere più di te

Nel 2033, 33

Non vedrò più con gli occhi miei

Ci saranno delle immagini che

Un altro mondo mi darà

Caterina Caselli, *Nel 2023* (1969)

1. Introduzione

L'articolo esamina l'uso della sorveglianza biometrica come una tecnologia preoccupante che incide negativamente su una serie di diritti umani fondamentali, tra cui il diritto alla privacy, alla libertà di movimento, al diritto di lasciare qualsiasi Paese, alla libertà di pensiero, coscienza e religione, alla libertà di opinione ed espressione, e alla libertà di riunirsi pacificamente. L'articolo esplora anche come i diritti umani siano concepiti in maniera diversa tra i due Paesi, contribuendo a comprendere le ragioni per cui le tecnologie di sorveglianza biometrica interferiscano con il diritto alla privacy e con altri diritti umani universali, come sancito nell'articolo 17 della "Convenzione internazionale sui diritti civili e politici" e nell'articolo 12 della "Dichiarazione universale dei diritti umani". Si approfondiranno come casi studio il sistema di sorveglianza delle frontiere in Canada, le violazioni dei diritti umani nello Xinjiang e l'ampio utilizzo del Sistema di Credito Sociale (SCS) in Cina. Le seguenti domande di ricerca vengono esplorate:

RQ1: La sorveglianza biometrica ha un impatto sui diritti umani fondamentali?

RQ2: In che misura le tecnologie biometriche stanno influenzando i diritti umani fondamentali in Cina e Canada?

La comparazione tra Repubblica Popolare Cinese e Canada non si limita ad un accostamento di casi geograficamente distanti, ma adotta un protocollo metodologico basato sulla valutazione di tre dimensioni chiave: le norme (analisi della PIPL cinese vs la legislazione federale canadese), la prassi operative (il Sistema di Credito Sociale e la sorveglianza delle frontiere) e l'enforcement (l'effettiva capacità dei cittadini di ricorrere contro gli abusi).

L'ipotesi di fondo è che le tecnologie biometriche non siano strumenti neutri, ma amplificatori dei modelli preesistenti di relazione tra Stato ed individuo: in Cina esse sono specchio di un paradigma statale nel quale la sorveglianza è un'estensione del potere governativo e non richiede giustificazione proporzionale; in Canada, invece, le stesse tecnologie mettono sotto pressione un sistema costituzionale di garanzie che tuttavia dispone di strumenti istituzionali – e.g. *Privacy Commissioner*, controllo giudiziario, società civile attiva – per contrastare e reagire. La comparazione non serve dunque a giustapporre due realtà geograficamente distanti, ma è il modello istituzionale e costituzionale preesistente a determinare se la biometria diventi uno strumento di oppressione o resti un rischio contenibile.



2. Cosa si intende per sorveglianza biometrica?

Prima di tutto, è essenziale definire il concetto di sorveglianza. Il termine può essere scomposto nella sua etimologia: *sur* (dall'alto) e *veillance* (guardare). Il significato letterale del termine è «l'attività di vigilare sulle persone»¹. Lyon definisce la sorveglianza come «la raccolta e l'elaborazione di dati personali, identificabili o meno, con l'obiettivo di influenzare o gestire coloro i cui dati sono stati raccolti»². Gary T. Marx descrive la sorveglianza come un «processo sociale fondamentale, caratteristico di tutte le società, sia funzionale che rischioso»³. Secondo Lyon⁴, «la sorveglianza non è né intrinsecamente buona né cattiva», ma è il contesto e il comportamento che le conferiscono un carattere positivo o negativo. Opere distopiche come *1984* di George Orwell, *Il Castello* di Franz Kafka o *Il racconto dell'ancella* di Margaret Atwood hanno messo in luce le minacce derivanti da un controllo statale opprimente. Fino a tempi relativamente recenti, non esistevano studi sistematici sulla sorveglianza. Sebbene quest'ultima fosse stata oggetto di studio, era trattata in modo isolato, frammentato e non sistematico. Negli ultimi venti anni, in particolare dopo gli attacchi dell'11 settembre, gli studi sulla sorveglianza hanno suscitato maggiore attenzione sia accademica che pubblica. Nonostante non siano emerse «scuole di pensiero» consolidate, l'esplosione di interesse ha aperto nuove possibilità al fine di comprendere meglio il fenomeno⁵.

Tra i teorici più importanti che elaborano cornici teoriche alternative al panoptismo possiamo menzionare la «società del controllo» (*control societies*) di Deleuze e Guattari, «l'assemblaggio sorvegliante» (*surveillant assemblage*) di Haggerty ed Ericson, e «il capitalismo della sorveglianza» (*surveillance capitalism*) di Zuboff⁶.

La neomarxista Zuboff, in *Surveillance Capitalism* offre un'analisi sistematica di come la sorveglianza pervasiva stia ridefinendo le strutture di potere nell'economia dell'informazione contemporanea⁷. L'autrice individua nel capitalismo della sorveglianza una forma inedita di accumulazione economica, il cui meccanismo fondamentale consiste nell'estrazione, nell'elaborazione e nella monetizzazione dei dati comportamentali degli individui con il fine ultimo di anticipare e orientare le scelte umane per generare profitto e consolidare il controllo del mercato. Zuboff lo definisce come: «A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales. A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioural modification»⁸.

Di conseguenza, il mercato non è più una forza economica sconosciuta come nel liberalismo classico, ma è visibile, inequivocabile e conoscibile in modi nuovi. Zuboff identifica tre caratteristiche di questo nuovo

¹ J. LEIBOLD, *Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement*, in *Journal of Contemporary China*, 121, 2019, 48.

² D. LYON, *Surveillance and Social Sorting: Privacy, Risk and Digital Discrimination*, London, 2003, 37-38.

³ G.T. MARX, *Surveillance Studies*, in J.D. WRIGHT (a cura di), *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, Cambridge (MA), 2015, 733-741.

⁴ D. LYON, *The Electronic Eye: The Rise of the Surveillance Society*, Minneapolis (MN), 1994, 5.

⁵ K. BALL, K. HAGGERTY, D. LYON (a cura di), *Routledge Handbook of Surveillance Studies*, 2012.

⁶ M. GALIĆ, T. TIMAN, B.-J. KOOPS, *Bentham, Deleuze and beyond: An Overview of Surveillance Theories from the Panopticon to Participation*, in *Philosophy & Technology*, 1, 2016, 9-37, 11.

⁷ S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019, 9.

⁸ *Ibid.*

modello economico. In primo luogo, l'interesse per i big data. In particolare, conia i termini *formal indifference* ("indifferenza formale")⁹ e *structural independence* ("indipendenza strutturale")¹⁰. Nell'*indifferenza formale*, l'estrazione dei dati avviene in assenza di qualsiasi forma di discussione o consenso informato da parte degli utenti, determinando una profonda asimmetria nel processo di raccolta e valorizzazione delle informazioni personali. L'*indipendenza funzionale* segna una rottura netta rispetto al paradigma aziendale novecentesco. Mentre quest'ultimo era fondato su reciprocità strutturali — carriere stabili, rapporti fiduciari duraturi con i consumatori, obblighi di lealtà reciproca — le grandi piattaforme tecnologiche organizzano i propri servizi, la gestione del personale e le relazioni con gli *stakeholder* attorno alla logica algoritmica, svuotando qualsiasi reciprocità. Ne consegue una personalizzazione sempre più sofisticata dell'offerta, capace di anticipare i bisogni dell'utente prima ancora che questi ne abbia consapevolezza, con effetti di significativo squilibrio informativo nel rapporto tra individuo e piattaforma. La terza caratteristica riguarda la capacità dell'infrastruttura tecnologica di penetrare nelle sfere più intime della vita degli utenti. Un caso emblematico, documentato e oggetto di accese polemiche, è il tentativo di Facebook di manipolare lo stato emotivo dei propri utenti attraverso la modulazione algoritmica dei contenuti del news feed, senza alcuna informazione o consenso preventivo¹¹. Zuboff definisce questo tipo di potere "instrumentarianism", ovvero «the instrumentation and instrumentalisation of behaviour for modification, prediction, monetisation, and control» ("la strumentazione e la strumentalizzazione del comportamento per la sua modificazione, previsione, monetizzazione e controllo")¹².

I marcatori biometrici sono tra i dati personali più distintivi, in quanto unici per ogni individuo. Le impronte digitali sono probabilmente il tipo di dato biometrico più noto e diffuso¹³. Tuttavia, oggi, grazie ai progressi tecnologici, si è in grado di raccogliere e monitorare anche dati biometrici più recenti come il riconoscimento vocale, facciale e retinico. Diverse forme di sorveglianza biometrica stanno diventando sempre più comuni in spazi pubblici ad alta affluenza, come centri commerciali, stadi, banche, aeroporti e mezzi di trasporto, soprattutto in luoghi con elevata densità di popolazione. Un esempio è il programma *Physicals for All* in Xinjiang, che raccoglie informazioni biometriche di quasi undici milioni di cittadini della regione¹⁴. Le tecnologie biometriche non costituiscono un blocco unico, ma presentano rischi differenziati per i diritti fondamentali a seconda delle loro caratteristiche tecniche e modalità di impiego. È quindi necessario distinguere innanzitutto tra identificazione (1:N) e verifica (1:1). Mentre la verifica (confronto tra il dato biometrico e un singolo modello memorizzato, es. blocco dello smartphone) ha un impatto limitato sulla privacy, l'identificazione (confronto "uno-a-molti per rintracciare un individuo tra la folla) trasforma lo spazio pubblico in un luogo di sorveglianza. Sotto il profilo temporale, la distinzione tra sistemi in tempo reale (*real-time*) e differiti (*post-event*) è fondamentale: i primi consentono un intervento immediato e potenzialmente discriminatorio, incidendo in modo diretto sulla libertà di riunione pacifica e di espres-

⁹ Ivi, 237.

¹⁰ Ivi, 314.

¹¹ R. BOOTH, *Facebook reveals news feed experiment to control emotions*, in *The Guardian*, 30, 2014, 2014.

¹² S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019, 223-224.

¹³ H.A. ÜNVER, *Politics of Digital Surveillance, National Security and Privacy*, Centre for Economics and Foreign Policy Studies, 2018, 6.

¹⁴ *Ibid.*

sione, dissuadendo la partecipazione civica attraverso un *chilling effect* o “congelamento dei diritti”¹⁵. I secondi, operando su materiale già acquisito, consentono una ricostruzione retroattiva dei movimenti, delle frequentazioni e delle abitudini di vita dei soggetti interessati, determinando una forma di sorveglianza posticipata che può rivelarsi altrettanto invasiva nella sfera privata dell'individuo. Se i database pubblici sono soggetti (almeno nelle democrazie) a vincoli di finalità e proporzionalità, l'integrazione con database privati espone i cittadini al rischio di *function creep*, ossia l'impiego delle tecnologie biometriche per scopi diversi da quelli dichiarati originariamente¹⁶.

Le tecnologie biometriche sollevano numerose criticità dal punto di vista dei diritti fondamentali¹⁷. In primo luogo, esse incidono sul diritto alla protezione dei dati personali e sul diritto alla vita privata, diritti che nelle democrazie costituzionali europee trovano tutela tanto a livello costituzionale quanto sovranazionale (art. 8 CEDU e artt.7-8 dei diritti fondamentali dell'UE). L'impiego di sistemi di riconoscimento facciale in spazi pubblici, soprattutto in tempo reale, riduce drasticamente le aspettative di anonimato, ma soprattutto rischia di avere forti ripercussioni sulla libertà di riunione pacifica e sulla libertà di espressione, dissuadendo di conseguenza la partecipazione civica. In secondo luogo, il già menzionato *function creep*, rappresenta un ulteriore pericolo. Un esempio significativo proviene dalle proteste seguite all'uccisione di George Floyd nel 2020: diversi dipartimenti di polizia statunitensi hanno utilizzato sistemi di riconoscimento facciale, inclusi quelli basati su database commerciali come *Clearview AI*, per identificare manifestanti e attivisti, nonostante non vi fossero reali minacce alla sicurezza pubblica tali da giustificare forme così invasive di monitoraggio¹⁸. In terzo luogo, la tecnologia biometrica potrebbe esacerbare disuguaglianze razziali, etniche, di genere e sociali, rafforzando processi di esclusione¹⁹. Tali tecnologie mettono in discussione l'effettività delle garanzie giuridiche. Mobilio evidenzia come il riconoscimento facciale, per la sua capacità di rendere l'identificazione automatica, remota e di massa, ponga sfide regolative senza precedenti: dalla necessità di definire limiti chiari all'uso delle basi dati, alla distinzione tra identificazione in tempo reale e post-evento, fino al problema della proporzionalità rispetto agli scopi perseguiti.

¹⁵ B. HARRIS, C. MURRAY, *Facial Recognition Technology in Policing and Security – Case Studies in Regulation*, in *Laws*, 13(3), 2024, 35.

¹⁶ V. NAJIBI et al., *Beyond Surveillance: Privacy, Ethics, and Regulations in Face Recognition Technology*, in *Frontiers in Artificial Intelligence*, 2024.

¹⁷ La regolamentazione di tali tecnologie è complessa, in quanto manca una definizione condivisa di “biometria”. L'Organizzazione Internazionale per la Standardizzazione (ISO) la definisce come “il riconoscimento automatizzato degli individui basato sulle loro caratteristiche biologiche e comportamentali” (ISO/IEC 2382-37). A livello europeo, i “dati biometrici” sono inclusi nella categoria dei “dati sensibili” ai sensi del “Regolamento Generale sulla Protezione dei Dati” (GDPR) come i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (Articoli 4(14) GDPR). Le caratteristiche fisiche considerate come possibili identificatori biometrici includono la lunghezza delle dita, la topografia della mano, le vene dei polsi e delle mani, le pieghe delle nocche, la forma delle orecchie e delle labbra; inoltre, i modelli vocali, le scansioni della retina, il riconoscimento dell'iride e della firma (Smith e Brooks 2013, 153).

¹⁸ S.M. SMYTH, *Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control*, London, 2019, 78.

¹⁹ V.L. COLELLA, *Biometric Surveillance during Protests: A Security Matter or a Violation of Human Rights?*, in *ITSS Verona Magazine*, 2(2), 2023.

²⁰ S.M. SMYTH, *Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control*, cit., 78.

L'adozione di tecniche biometriche, pertanto, non incide solo sulla sfera privata sugli individui, ma tocca l'intero equilibrio tra potere pubblico, libertà personale e partecipazione democratica²⁰.

3. La concezione dei diritti umani in Asia e in Occidente

Nel nostro linguaggio quotidiano, "Asia" si riferisce a una vasta regione geografica, che ospita numerosi Stati e i loro cittadini, tutti caratterizzati da culture, religioni, economie e sistemi politici radicalmente diversi. L'enorme diversità dell'Asia rende impossibile sostenere l'esistenza di valori asiatici comuni²¹.

Il dibattito sull'universalità dei diritti umani è stato caratterizzato, a partire dagli anni Novanta, da posizioni critiche che mettono in discussione l'assetto della legislazione internazionale, talvolta descritta come eccessivamente legata ad una matrice liberale di stampo eurocentrico, e dunque ritenuta da alcuni attori politici poco aderente alle specificità del Sud globale. In particolare, alcuni governi del Sud-est asiatico – tra cui spiccano le posizioni storiche di Singapore, Malaysia e Indonesia – hanno promosso la retorica dei cosiddetti "valori asiatici". Secondo questa costruzione politica e argomentativa, gli standard internazionali dei diritti umani non sarebbero pienamente rappresentativi delle strutture sociali locali, spesso associate nel discorso ufficiale a una presunta eredità confuciana centrata sull'armonia collettiva e sulla stabilità sociale, piuttosto che sulle prerogative individuali²². Inoltre, vi sono anche altre voci da considerare, tra cui quelle dei popoli indigeni, dei gruppi svantaggiati e oppressi, insieme alla crescente voce delle classi medie²³.

Tutte queste questioni furono discusse alla Conferenza Mondiale delle Nazioni Unite sui Diritti Umani del 1993 a Vienna. La Conferenza approvò la Dichiarazione di Vienna e il Piano d'Azione il 25 giugno 1993, che comprendevano 39 "paragrafi" (il termine utilizzato al posto di "principi", ritenuto inaccettabile da alcuni delegati) e un "programma d'azione"²⁴. L'obiettivo principale era riaffermare l'universalità dei diritti umani: «All human rights are universal, indivisible and interdependent and interrelated. The international community must treat human rights globally fairly and equally, on the same footing, and with the same emphasis»²⁵.

Sebbene la Dichiarazione di Vienna ribadisca che i diritti umani si applicano a tutti, essa sottolinea anche la necessità di considerare le specificità regionali.²⁶ La Conferenza – che riuscì a ottenere un ampio consenso dopo quarantacinque anni dalla DUDU – fu convocata principalmente in risposta a una dichiarazione regionale pre-conferenza nota come *Bangkok NGO Declaration on Human Rights* (1993), nella quale il dibattito sui "valori asiatici" raggiunse il suo apice. Il Rapporto, firmato da oltre quaranta nazioni asiati-

²⁰ G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, 57.

²¹ L. XIAORONG, "Asian Values" and the Universality of Human Rights, in *Philosophy and Public Policy Quarterly*, 2, 1996, 19.

²² K. ENGLE, *Culture and Human Rights: The Asian Values Debate in Context*, in *NYUJ Int'l L. & Pol.*, 32, 1999, 311.

²³ Y. GHAI, *Asian Perspectives on Human Rights*, in *Hong Kong Law Journal*, 23, 1993, 343.

²⁴ C.M. CERNA, *Universality of Human Rights and Cultural Diversity: Implementation of Human Rights in Different Socio-Cultural Contexts*, in *Human Rights Quarterly*, 16, 1994, 741.

²⁵ World Conference on Human Rights, *Vienna Declaration and Programme of Action*, Vienna, 25 June 1993. Tutti i diritti umani sono universali, indivisibili, interdipendenti e correlati. La comunità internazionale deve trattare globalmente i diritti umani in modo giusto ed equo, sullo stesso piano e con la stessa enfasi. (Par. 1.5, 3).

²⁶ C.M. CERNA, *Ivi*, 749.

che, criticava l'attuale quadro dei diritti umani e chiedeva, tra le altre cose, che si tenesse conto degli aspetti storici, culturali e religiosi peculiari della regione²⁷. Il Preambolo della *Final Declaration of the Regional Meeting for Asia of the World Conference on Human Rights* riporta che: «Recognising the contribution that can be made to the World Conference by Asian countries with their diverse and rich cultures and traditions and [...] that the promotion of human rights should be encouraged by cooperation and consensus, and not through confrontation and the imposition of incompatible values (1993, 3)»²⁸.

In risposta a tali rivendicazioni, il governo degli Stati Uniti respinse l'idea che la definizione dei diritti umani potesse essere condizionata dalle specificità regionali, riaffermandone il carattere universale e indivisibile. Da questa prospettiva, l'argomento della "differenza culturale" venne interpretato come un espediente retorico utilizzato da alcuni governi asiatici per sottrarre i propri regimi autoritari allo scrutinio internazionale. Specularmente, diverse delegazioni di governi asiatici sostennero la tesi della "gradualità": secondo questa visione, il godimento dei diritti civili e politici sarebbe subordinato al raggiungimento di una soglia minima di sviluppo economico. A sostegno di ciò, durante la Conferenza di Vienna del 1993, la delegazione cinese pose l'accento sul diritto allo sviluppo come preconditione indispensabile, citando la povertà come il principale ostacolo al pieno esercizio delle libertà fondamentali. In tale ottica, l'universalità dei diritti risulterebbe priva di sostanza se non preceduta dalla stabilità sociale e dalla crescita economica, intese come basi materiali necessarie per l'effettività di qualsiasi garanzia giuridica²⁹. Una posizione ancora più forte è adottata da Bilahari Kausikan, uno dei primi sostenitori dei valori asiatici ed ex direttore dell'Ufficio per l'Asia orientale e il Pacifico del Ministero degli Esteri di Singapore. Egli sostenne come la cooperazione internazionale dovrebbe concentrarsi prioritariamente sul nucleo dei diritti definiti come inderogabili e riconosciuti come *jus cogens* (quali il divieto di genocidio, di tortura o di crimini contro l'umanità)³⁰.

Un esempio emblematico di questa visione è rappresentato dalle tesi dell'ex Primo Ministro di Singapore, Lee Kuan Yew. Durante l'Asahi Forum del 1992, Lee difese le politiche del suo Paese sostenendo che l'enfasi eccessiva sui diritti individuali – osservata in alcuni contesti occidentali – avrebbe condotto ad un indebolimento del tessuto civile. Citando fenomeno di marginalità e criminalità come prova di una crisi dei modelli individualisti, Lee argomentò che la priorità di un governo deve essere la garanzia di una società sicura. Solo all'interno di un quadro sociale stabile e ben organizzato, l'individuo può effettivamente beneficiare delle proprie libertà³¹.

Infine, i diritti umani riguardano la sovranità nazionale. Il paragrafo 5 sottolinea il rispetto della sovranità nazionale, dell'integrità territoriale e della non-ingerenza negli affari interni degli altri Stati, così come l'uso dei diritti umani come strumento di pressione politica³². L'autorità interna di un governo in materia di diritti umani è una componente del diritto all'autodeterminazione di una nazione. I governi stranieri o

²⁷ K. ENGLE, *op. cit.*, 311.

²⁸ Ministers And Representatives Of Asian States, *Final Declaration of the Regional Meeting for Asia of the World Conference on Human Rights (Bangkok Declaration)*, New York, 1993. «Riconoscendo il contributo che può essere dato alla Conferenza Mondiale dai Paesi asiatici con le loro culture e tradizioni diversificate e ricche e [...] che la promozione dei diritti umani dovrebbe essere incoraggiata attraverso la cooperazione e il consenso, e non tramite il confronto e l'imposizione di valori incompatibili (1993, 3)».

²⁹ C.M. CERNA, *op. cit.*, 319.

³⁰ B. KAUSIKAN, *Asia's Different Standard*, in *Foreign Policy*, 92, 1993, 24-41.

³¹ K. ENGLE, *op. cit.*, 320.

³² M.C. DAVIS, *Chinese Perspectives on the Bangkok Declaration and the Development of Human Rights in Asia*, in *Proceedings of the ASIL Annual Meeting*, 89, 1995, 163.

le organizzazioni internazionali non dovrebbero interferire nelle questioni interne, compresi i diritti umani. La Cina, nel suo Libro Bianco del 1991, affermava che la questione dei diritti umani rientra in larga misura nella sovranità di ciascuno Stato³³.

4. Breve storia della legislazione cinese sulla privacy

In Cina, il concetto di privacy ha subito una trasformazione significativa³⁴. In cinese, il termine “privacy” non è più limitato alla vecchia e rigorosa definizione di Yinsi (隐私), intesa come un “segreto vergognoso”; piuttosto, ora si riferisce a tutte le informazioni personalmente identificabili (vergognose o meno) che una persona non desidera siano conosciute da altri³⁵.

Sebbene la legge cinese abbia esplicitamente riconosciuto la privacy come un diritto autonomo solo nel 2021³⁶, dal 1980 in poi la protezione legale dei diritti personali è aumentata progressivamente. Secondo i dati dell’Internet Society of China, il 54% degli utenti internet cinesi ritiene che le violazioni della privacy siano un problema serio³⁷.

L’articolo 38 della Costituzione sancisce che la dignità personale dei cittadini della RPC è inviolabile: un cittadino non può essere insultato, diffamato, accusato falsamente né avere la propria reputazione “compromessa” in alcun modo³⁸. Gli articoli 37 e 39 proteggono la libertà della persona e della residenza. La Costituzione cinese prevede, agli articoli 40, 51, 53 e 54, un sistema articolato di limitazioni ai diritti fondamentali. Emergono infatti clausole di portata assai più ampia, formulate in termini sufficientemente elastici da consentire allo Stato di invocarle a sostegno di strumenti di controllo sociale come il sistema di credito sociale, subordinando in tal modo l’esercizio dei diritti individuali alla protezione degli interessi collettivi e dell’ordine statale. Ad esempio, l’articolo 40 tutela la privacy della corrispondenza, «tranne nei casi in cui, per soddisfare le esigenze della sicurezza dello Stato o delle indagini penali, gli organi di pubblica sicurezza o quelli della procura siano autorizzati a esaminare la corrispondenza secondo le procedure previste dalla legge»³⁹. L’articolo 51 afferma che: «Citizens of the People’s Republic of China, in exercising their freedoms and rights, must not infringe upon the interests of the State, of society, or of the collective, or upon the lawful freedoms and rights of other citizens»⁴⁰.

³³ S. SCEATS, S. BRESLIN, *China and the International Human Rights System*, London, 2012, 21.

³⁴ LÜ YAO-HUAI, *Privacy and Data Privacy Issues in Contemporary China*, in *Ethics and Information Technology*, 7(1), 2005, 7.

³⁵ I. CALZADA, *Citizens’ Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*, in *Smart Cities*, 5(3), 2022, 1133.

³⁶ Il Codice Civile cinese del 2021 (entrato in vigore il 1° gennaio 2021) ha dedicato per la prima volta un intero libro ai “diritti della personalità”, includendo espressamente il diritto alla privacy (*yǐnsī quán*, 隐私权) come diritto civile autonomo e tutelato. L’articolo 1032 definisce la privacy come “la pace della vita privata di una persona fisica e lo spazio privato, le attività private e le informazioni private che non desidera che altri conoscano”.

³⁷ W. YANG, *How Much Do Chinese People Care about Privacy?* – DW – 04/12/2018, 13 aprile 2018.

³⁸ Y.-H. LÜ, *Privacy and Data Privacy Issues in Contemporary China*, in *Ethics and Information Technology*, 7(1), 2005, 7-15.

³⁹ Costituzione della Repubblica Popolare Cinese, 2004, art. 10.

⁴⁰ Costituzione della Repubblica Popolare Cinese, 2004, art. 10. «I cittadini della Repubblica Popolare Cinese, nell’esercizio delle loro libertà e dei loro diritti, non devono ledere gli interessi dello Stato, della società o della collettività, né le libertà e i diritti legittimi di altri cittadini» (*Ibid.*, 11).



Sia il Codice civile “de facto” cinese, ossia i Principi generali del diritto civile del 1986, sia il Codice penale della Repubblica Popolare Cinese del 1997 non contemplano il termine “privacy”. Essi fanno invece riferimento alla “reputazione” (art. 221), applicabile tanto ai cittadini quanto alle persone giuridiche. L'introduzione del diritto alla privacy nel quadro giuridico cinese avviene soltanto nel 2009, con l'adozione della Legge sulla responsabilità civile per illeciti, che attribuisce alla privacy un valore giuridico equivalente a quello della reputazione⁴¹. Tale equiparazione deriva dal riconoscimento della privacy come “diritto della personalità”, categoria che include, tra gli altri, il diritto alla vita e alla salute, il diritto al nome e all'immagine, nonché i diritti reputazionali⁴².

L'intelligenza artificiale (AI) e l'Internet delle cose (IoT) stanno diventando componenti sempre più integrate nella vita quotidiana dei consumatori, grazie ai progressi tecnologici maturati nell'ecosistema dei Big Data. Un impulso determinante a questa trasformazione è stato fornito dal Tredicesimo Piano Quinquennale per lo Sviluppo Economico e Sociale della Repubblica Popolare Cinese (13° PQ), approvato dalla Quarta Sessione Plenaria del 12° Congresso Nazionale del Popolo nel marzo 2016, che ha rafforzato in modo significativo il sostegno politico al settore delle tecnologie dell'informazione e della comunicazione (ICT). Nello stesso anno, il Ministero dell'Industria e della Tecnologia dell'Informazione ha pubblicato il Piano per lo Sviluppo dei Big Data, delineando una strategia che, entro il 2020, mirava a raggiungere risultati sostanziali nella costruzione della cosiddetta “Cina Digitale”⁴³.

Parallelamente, l'attuazione di queste strategie comporta una serie di rischi, in particolare in relazione alla tutela della privacy dei dati personali. L'evoluzione delle tecnologie ICT tende infatti a conferire al governo e alle imprese tecnologiche capacità sempre più avanzate di monitorare e profilare su vasta scala la popolazione. In questo contesto, l'adozione da parte del governo cinese di pratiche di sorveglianza particolarmente stringenti ha portato a descrivere la Regione Autonoma Uigura dello Xinjiang come un vero e proprio “laboratorio di sorveglianza ad alta tecnologia”⁴⁴. Mentre, il Sistema di Credito Sociale è probabilmente la riforma che ha l'impatto maggiore sul diritto alla privacy⁴⁵.

Negli ultimi anni, la Repubblica Popolare Cinese ha intensificato gli sforzi volti alla creazione di un quadro legislativo coerente per la protezione dei dati personali, culminati nell'agosto 2021 con l'adozione della Legge sulla Protezione delle Informazioni Personali (PIPL). Questa normativa può essere interpretata come una “terza via” rispetto al modello statunitense, orientato al mercato, e all'approccio europeo, maggiormente incentrato sulla tutela della privacy. La PIPL definisce le informazioni personali come «qualsiasi tipo di informazione relativa a persone fisiche identificate o identificabili, registrata elettronicamente o con altri mezzi, esclusi i dati resi anonimi» (Art. 4)⁴⁶.

La PIPL persegue quattro obiettivi principali: proteggere i cittadini da pratiche di raccolta e utilizzo dei dati considerate non etiche o inappropriate da parte delle imprese; promuovere la crescita dell'economia digitale; tutelare l'“interesse pubblico” così come definito dalle autorità di Pechino; e rafforzare la reputa-

⁴¹ Y. FENG, *The Future of China's Personal Data Protection Law: Challenges and Prospects*, in *Asia Pacific Law Review*, 27, 1, 2019, 69.

⁴² R. CREEMERS, *China's emerging data protection framework*, in *Journal of Cybersecurity*, 8(1), 2022, 3.

⁴³ *Ivi*, 66.

⁴⁴ Y. FENG, *op. cit.*, 67.

⁴⁵ F. 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 & Internet*, 10(4), 2018, 415.

⁴⁶ R. CREEMERS, *op. cit.*, 1.

zione internazionale della Cina in materia di sicurezza dei dati, favorendo al contempo la cooperazione globale sui flussi transfrontalieri di informazioni personali. La normativa non introduce diritti fondamentali o principi giuridici universali, ma regola in maniera estremamente dettagliata i diversi attori e le loro interazioni, partendo dai rischi o dai potenziali danni percepiti che tali pratiche possono generare. Pur rappresentando, insieme alla *Legge sulla Cybersecurity* (CSL) e alla *Legge sulla Sicurezza dei Dati* (DSL), un passo significativo verso la tutela delle informazioni personali, l'effettiva applicazione della PIPL risulta ancora limitata⁴⁷.

Sebbene la legislazione preveda esplicitamente restrizioni alla raccolta eccessiva di dati (Art. 6), all'impiego di processi decisionali automatizzati (Art. 24) e al trattamento delle informazioni personali dei minori (Art. 31), e disponga di un'ampia gamma di strumenti di enforcement – tra cui sanzioni pecuniarie, procedimenti amministrativi, richieste di risarcimento e contenziosi giudiziari – essa continua comunque a consentire l'utilizzo delle informazioni personali nell'ambito di rilevanti programmi statali. Tra questi figurano il Sistema di Credito Sociale (SCS) e le attività di raccolta e trattamento dei dati funzionali agli obiettivi operativi delle agenzie di sicurezza interna e delle forze di polizia⁴⁸.

Le esigenze di tutela della privacy introdotte dalla PIPL possono essere pienamente comprese solo considerando il profondo impatto esercitato dal Sistema di Credito Sociale (SCS) sui cittadini e il crescente sviluppo di un regime di "cittadinanza cibernetica", fenomeno che si è intensificato nella Cina post-pandemica. In particolare, il SCS è stato impiegato per adattare la governance durante la pandemia, consentendo un monitoraggio capillare dei comportamenti individuali⁴⁹.

Tuttavia, la PIPL e gli altri quadri normativi attualmente vigenti risultano spesso troppo ambigui o eccessivamente generici. La PIPL, ad esempio, non fornisce indicazioni specifiche su come gestire l'archiviazione dei dati biometrici sensibili, quale tipo di crittografia debba essere adottato, né su chi debba essere responsabile degli audit dei dati, della definizione delle regole o dell'applicazione della legge.

4.1. Il Sistema di Credito Sociale (SCS): impatto sui diritti umani fondamentali

Il Sistema di Credito Sociale (SCS) è una rete di meccanismi di controllo dell'affidabilità per persone fisiche e giuridiche, basata su osservazione, registrazione, penalizzazioni e premi. Introdotto nel 2014, è diventato pienamente operativo nel 2020 per l'intera popolazione cinese⁵⁰. Sulla base dei risultati delle informazioni raccolte, le persone vengono inserite nella lista rossa (premi) o nella lista nera (punizioni e sanzioni)⁵¹. *Credit China* pubblica e aggiorna regolarmente le "liste nere" e "rosse" di individui e organizzazioni sul proprio sito web⁵². Il SCS è considerato un elemento fondamentale per realizzare "il Sogno Cinese" –

⁴⁷ I. CALZADA, *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*, in *Smart Cities*, 5(3), 2022, 1135.

⁴⁸ R. CREEMERS, *op. cit.*, 6.

⁴⁹ I. CALZADA, *op. cit.*, 1132.

⁵⁰ J. PABISIAK, *Dangerous, Yet Not So Unique. Characteristics of the Chinese Social Credit System*, in *Polish Political Science Yearbook*, 49(3), 2020, 30.

⁵¹ K. YU, *Towards Graduated Citizenship: A Study of Social Credit Systems in China*, in *Critique: a Worldwide Student Journal of Politics*, 2020, 35.

⁵² O.O. BAZINA, *Human Rights and Biometric Data. Social Credit System*, in *Przegląd Europejski*, 2020, 4(58), 47.



il progetto di Xi Jinping – al fine di rafforzare i “valori socialisti”⁵³. Tuttavia, questo sistema non è compatibile con gli standard internazionali sui diritti umani, come il diritto a non essere soggetti a invasioni arbitrarie della propria privacy, famiglia, casa o corrispondenza; il diritto a non essere discriminati; il diritto alla libertà di opinione ed espressione; il diritto alla libertà di movimento, e altri diritti ad essi strettamente correlati. Raghunath sostiene che il SCS influenzi negativamente il successo occupazionale, poiché interagisce con le reti (*guanxi*), ostacolando così gli sforzi per migliorare la mobilità sociale ed etichettando alcune persone come ad alto rischio⁵⁴. In Cina, le relazioni amicali esercitano un’influenza maggiore sui processi di ricerca del lavoro rispetto ai paesi occidentali, dove prevalgono i legami deboli⁵⁵. Inoltre, i *guanxi* sono strettamente legati all’idea di credibilità e affidabilità (*xinyong*)⁵⁶. A causa della fiducia percepita, le valutazioni del credito sociale influenzano significativamente la capacità delle persone di svolgere il proprio lavoro e di cercarne uno. Ad esempio, il personale ospedaliero afferma che alcune amministrazioni locali abbiano stabilito soglie minime di valutazione del credito sociale per l’occupazione⁵⁷. Ciò mette a rischio il diritto al lavoro (art. 23) sancito dalla Dichiarazione Universale dei Diritti Umani.

Le valutazioni dei cittadini cinesi sono suddivise in quattro categorie, da “A” a “D”: “A” indica affidabilità, “B” onestà, “C” irresponsabilità e “D” inaffidabilità. A seconda del punteggio ottenuto, i cittadini ricevono trattamenti differenti e hanno accesso a opportunità sociali limitate. I residenti con un punteggio “A” possono ottenere lavori di qualità, accedere al servizio civile, prendere voli, soggiornare in hotel e iscrivere i propri figli in scuole rinomate, oltre ad usufruire di vantaggi in termini di occupazione, indennità giornaliera e supporto sociale⁵⁸. Al contrario, le persone con un punteggio “D” sono emarginate dalla società: non vengono assunte, non ricevono prestiti, non possono acquistare biglietti aerei o ferroviari (soprattutto i treni ad alta velocità) e non possono noleggiare un’auto⁵⁹. Di conseguenza, l’SCS compromette il diritto alla libertà di movimento e il diritto all’uguaglianza e alla non discriminazione (DUDU, art. 7).

Anche online, gli utenti non godono della privacy o dell’anonimato, poiché il *Grande Firewall* (Great Firewall) è incaricato di monitorare, eliminare e segnalare i contenuti “illegali”, minacciando il diritto alla libertà di opinione e di espressione (DUDU, art. 19). Il *Grande Firewall della Cina* è il nome con cui i media occidentali (il nome compare per la prima volta nella rivista *Wired* nel 1997) si riferiscono all’insieme di strumenti, servizi e normative adottati dal governo della Repubblica Popolare Cinese per bloccare determinati contenuti online all’interno dei confini nazionali. Implementato a partire dal 1996, il suo obiettivo principale è quello di impedire l’accesso a determinate informazioni che Pechino ritiene contrarie agli interessi del governo e della popolazione. A tal fine, il firewall blocca interi siti web e filtra i contenuti presenti su piattaforme non completamente oscure⁶⁰.

⁵³ T. LAM, *The People’s Algorithms: Social Credits and the Rise of China’s Big (Br)other*, in *The New Politics of Numbers: Utopia, Evidence and Democracy*, A. MENNICKEN & R. SALAIS (a cura di), Cham, 2022, 71.

⁵⁴ N. RAGHUNATH, *A Sociological Review of China’s Social Credit Systems and Guanxi Opportunities for Social Mobility*, in *Sociology Compass*, 14(5), 2020, 1.

⁵⁵ C. SU, J.E. LITTLEFIELD, *Entering Guanxi: A Business Ethical Dilemma in Mainland China?*, in *Journal of Business Ethics*, 33(3), 2001, 199.

⁵⁶ N. RAGHUNATH, *op. cit.*, 5.

⁵⁷ *Ivi*, 24.

⁵⁸ D.M. SÍTHIGH, M. SIEMS, *The Chinese Social Credit System: A Model for Other Countries?*, in *Modern Law Review*, 82(6), 2019, 1035.

⁵⁹ O.O. BAZINA, *op. cit.*, 45-46.

⁶⁰ S. KERNER, *Great Firewall of China*, TechTarget, 2022.



Inoltre, è stato dimostrato che è molto difficile far rimuovere un nome da una lista nera una volta che vi è stato inserito⁶¹, un processo che nell'UE è noto come "diritto all'oblio" (art. 17 del GDPR). Poiché i diritti umani sono interdipendenti e non possono essere considerati separatamente, il SCS rischia anche di compromettere il diritto alla salute. Infatti, chi ha un punteggio "A" può accedere ai trattamenti ospedalieri senza necessità di una garanzia, a condizione che il costo non superi i 10.000 yuan. Questa somma non garantita aumenta a ventimila e cinquantamila yuan per i punteggi "AA" e "AAA", rispettivamente. Le persone con punteggi più alti possono beneficiare di assistenza medica gratuita in ospedali o cliniche⁶².

4.2. La Regione Autonoma Uigura dello Xinjiang

La Regione Autonoma Uigura dello Xinjiang, situata nel nord-ovest della Repubblica Popolare Cinese (RPC) e confinante con Mongolia, Russia, Kazakistan, Kirghizistan, Tagikistan e Afghanistan, passa sotto il controllo definitivo del governo comunista cinese nel 1949. Sebbene gli Uiguri, di religione musulmana siano la maggioranza nella regione, la popolazione Han (il gruppo etnico prevalente in Cina) è in continuo aumento grazie a politiche che incentivano la migrazione verso quest'area⁶³. La minoranza musulmana uigura è oggetto di crescenti restrizioni e discriminazioni imposte dal Partito Comunista Cinese (PCC), che ha creato un sistema di sorveglianza senza precedenti nella Regione negli ultimi dieci anni. Questa sorveglianza statale include l'uso di strumenti tecnologicamente avanzati come il tracciamento GPS, il riconoscimento vocale e facciale, gli algoritmi di machine learning e altri software e hardware, oltre al monitoraggio fisico e alla sorveglianza forzata delle famiglie, che avviene non solo nelle abitazioni, ma anche nei "campi di rieducazione"⁶⁴.

Dal 2009, numerosi episodi di violenza hanno causato centinaia di morti e molti feriti. Tra gli incidenti principali si annoverano l'autoimmolazione a Pechino nell'ottobre 2013, l'attacco alla stazione ferroviaria di Kunming nel marzo 2014, l'attentato alla stazione ferroviaria di Ürümqi nell'aprile 2014 e al mercato della stessa città con veicoli ed esplosivi nel maggio 2014⁶⁵. Da allora, lo Xinjiang è stato definito il "campo di battaglia principale" della Cina nella lotta contro le "tre forze malvagie" (三个势力): terrorismo, estremismo e separatismo⁶⁶. Per contrastare l'attività criminale e terroristica, il PCC ha implementato un sistema di riconoscimento delle emozioni che «identifica segni di aggressività e nervosismo, nonché i livelli di stress e il potenziale di una persona di attaccare gli altri»⁶⁷. In questo modo, il governo mira a ottenere una "copertura totale", per evitare "zone cieche e aree vuote"⁶⁸. Più di un terzo delle comunità è sorvegliato da oltre 160.000 telecamere e 1.000 agenti di sicurezza. Ogni cittadino nello Xinjiang è obbligato a scaricare l'app di sicurezza *Cleannet Bodyguard* sui propri dispositivi personali: l'obiettivo di questo soft-

⁶¹ L. RETTINGER, *The Human Rights Implications of China's Social Credit System*, in *Journal of High Technology Law*, 21(1), 2022/2021, 25.

⁶² O.O. BAZINA, *op. cit.*, 46.

⁶³ M. LEE, E. YAZICI, *China's Surveillance and Repression in Xinjiang*, in *The Cambridge Handbook of Race and Surveillance*, a cura di M. KWET, Cambridge, 2023, 168.

⁶⁴ J. LEIBOLD, *Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement*, in *Journal of Contemporary China*, 29(121), 2019, 46.

⁶⁵ J. MILLWARD, D. PETERSON, *China's System of Oppression in Xinjiang: How It Developed and How to Curb It*, 2020, 3.

⁶⁶ J. LEIBOLD, *op. cit.*, 46.

⁶⁷ M. LEE, E. YAZICI, *op. cit.*, 183.

⁶⁸ J. LEIBOLD, *op. cit.*, 49.



ware è identificare automaticamente film, fotografie, *e-book* e documenti elettronici legati al terrorismo e alla religione illecita, avvisando le autorità competenti⁶⁹.

L'uso di tale applicazione e del riconoscimento delle emozioni fallisce il test di legalità e proporzionalità secondo gli standard internazionali: la base legale è generica (sicurezza nazionale) e la misura non è né strettamente necessaria né proporzionata rispetto allo scopo. L'eliminazione delle attività culturali, linguistiche e religiose non-Han, la riduzione degli spazi di autonomia, la mobilitazione sociale dal basso e il declino della fiducia sociale influenzano negativamente il diritto alla libertà di riunione pacifica e di associazione (art. 20 DUDU), nonché il diritto di partecipare liberamente alla vita culturale della comunità (art. 27 DUDU). Infine, anche l'equilibrio psicofisico delle persone è compromesso a causa degli abusi fisici e mentali sistematici. Gli ex detenuti uiguri raccontano di celle anguste, indottrinamento, torture, percosse durante gli interrogatori, privazioni di cibo e sonno come punizione, lunghe permanenze incatenati a sedie, scosse elettriche e altri abusi fisici e psicologici estremi⁷⁰. Anche l'articolo 26 della DUDU (diritto all'istruzione) viene sistematicamente violato poiché le famiglie vengono separate forzatamente, con i bambini inviati in orfanotrofi quando i genitori vengono internati in prigione o trasferiti in altre parti della Cina per ricevere un'istruzione obbligatoria. Inoltre, Pechino, attua il programma *Pair Up and Become Family*, inviando quadri (membri del PCC) a soggiornare regolarmente con famiglie musulmane e infiltrarsi nella loro vita privata allo scopo di integrarsi con la maggioranza Han. La durata delle visite può occasionalmente superare i cinque giorni, e i movimenti delle famiglie sono costantemente monitorati e sorvegliati⁷¹. Queste pratiche violano l'articolo 16 DUDU («Uomini e donne in età adatta hanno il diritto di sposarsi e di fondare una famiglia, senza alcuna limitazione di razza, cittadinanza o religione [...]). Dall'inizio del 2010, il governo cinese ha utilizzato tecnologie emergenti per ricercare ed esaminare frasi ritenute radicali, come "Corano" o "Allah", utilizzando tali espressioni come giustificazioni per detenere o imprigionare le persone in base alle loro convinzioni. Nel biennio 2017-2018, nello Xinjiang, oltre 350.000 persone sono state perseguitate, un dato che supera di gran lunga le meno di 30.000 registrate negli anni precedenti⁷². Questo contesto mette a rischio vari diritti umani, come il diritto alla libertà di pensiero, coscienza e religione (art. 18 DUDU), e il diritto alla libertà di opinione ed espressione (art. 19 DUDU). La Cina viola anche gli articoli 9 e 11 della DUDU, poiché detiene arbitrariamente persone nello Xinjiang per periodi di tempo illimitato, senza un processo giusto ed equo. Spesso, i familiari dei detenuti non riescono a comunicare con loro e potrebbero non sapere dove si trovano per anni⁷³. Per queste ragioni, il 19 gennaio 2021, la Cina è stata accusata di genocidio dal Segretario di Stato degli Stati Uniti, Mike Pompeo;⁷⁴ mentre un rapporto dell'ONU ha suggerito che le azioni potrebbero configurarsi come crimini contro

⁶⁹ *Ivi*, 52.

⁷⁰ G. O'CONNELL, *How China is Violating Human Rights Treaties and its Own Constitution in Xinjiang*, in *Just Security*, 19 agosto 2020, disponibile a: <https://www.justsecurity.org/> (ultimo accesso: 14 novembre 2024).

⁷¹ *Ibid.*

⁷² J. MILLWARD, D. PETERSON, *op. cit.*, 5.

⁷³ Per approfondire, consiglio la lettura del libro G. HAITIAJI, *Sopravvissuta a un gulag cinese*, settembre 2021.

⁷⁴ M. LEE, E. YAZICI, *op. cit.*, 166.

l'umanità⁷⁵. Secondo altre autorevoli organizzazioni internazionali, tra cui *Amnesty International* e *Human Rights Watch*, la Repubblica Popolare Cinese (RPC) viola la libertà e i diritti umani del popolo uiguro⁷⁶. Prima di analizzare il caso canadese è utile rendere esplicita la griglia comparativa citata nell'introduzione, mettendo a confronto i due sistemi sulle tre dimensioni chiave fin qui esaminate per la Cina. Sul piano delle *norme*, la PIPL cinese e la normativa canadese (*Privacy Act*, *PIPEDA*, *Canadian Charter*) entrambe richiamano finalità, proporzionalità e consenso – ma divergono radicalmente nella struttura: la PIPL deroga esplicitamente ai programmi statali, rendendo la tutela della privacy debole rispetto agli obiettivi di sicurezza nazionale e ordine sociale; la Charter canadese, al contrario, impone allo Stato di superare un test di proporzionalità (*Section 1*) anche quando invoca la sicurezza pubblica. Sul piano della prassi, entrambi i Paesi hanno costruito sistemi biometrici su larga scala – il SCS e lo Xinjiang da un lato, la sorveglianza aeroportuale dall'altro – ma con una differenza qualitativa decisiva: in Cina la sorveglianza biometrica è pervasiva, preventiva e rivolta alla popolazione nella sua totalità; in Canada essa è circoscritta a contesti specifici (frontiere, forze dell'ordine) e deve rispondere a criteri di necessità. Sul piano dell'*enforcement*, il divario è più netto: in Cina, l'assenza di un sistema giudiziario indipendente e la deroga esplicita della PIPL per i programmi statali rendono le istanze dei cittadini strutturalmente inefficaci; in Canada, il Privacy Commissioner ha dimostrato – con il caso *Clearview AI* – la capacità concreta di bloccare pratiche illegittime, imponendo il divieto operativo e la distruzione dei dati. È proprio sull'*enforcement* che la comparazione produce il suo risultato più significativo, come si argomenterà nelle conclusioni.

5. Il Canada e la sua legislazione sulla privacy

Il diritto alla privacy in Canada è tutelato attraverso una combinazione di strumenti, alcuni di natura costituzionale e altri basati su approcci legislativi o regolamentari.

L'analisi dell'impatto della sorveglianza biometrica in Canada non può prescindere da un rigoroso ancoraggio alla *Canadian Charter of Rights and Freedom* (1982). In particolare, l'uso di sistemi di riconoscimento facciale e scansione biometrica alle frontiere e negli spazi urbani solleva una frizione diretta con la *Section 8* della Carta, che garantisce il diritto alla protezione contro perquisizioni, sequestri o sequestri irragionevoli (*unreasonable search or seizure*). La giurisprudenza canadese ha stabilito che tale protezione si estende laddove vi sia una "ragionevole aspettative di privacy", un concetto che la prassi amministrativa sta faticosamente cercando di adattare alla persistenza dei dati biometrici⁷⁷. Sotto il profilo della prassi amministrativa, un punto di svolta fondamentale è rappresentato dalle indagini congiunte del *Privacy Commissioner of Canada* sul caso *Clearview AI*. In questo caso, l'autorità di controllo ha applicato rigorosamente il *Privacy Act* (per le istituzioni pubbliche) e il *PIPEDA* (per il settore privato), stabilendo che il *web scraping* di immagini facciali per finalità di sorveglianza da parte della Royal Canadian Mounted police (RCMP) costituisce una raccolta illegittima di informazioni personali. Questo evidenzia un modello di "enforcement attivo" che differisce radicalmente dal contesto cinese: la legalità del trattamento non è pre-

⁷⁵ A. HARRIS, *Until the United States Regulates Tech Exports, It Will Continue to Enable China's Surveillance of the Uyghurs*, in *Human Rights Brief*, 25(1), 2021, 58.

⁷⁶ A. ÇİÇEK, *Political Re-education Camps in Xinjiang as a Part of Panopticon-like Society: Clashing Discourses of Western and Chinese Media*, in *Wschodnioznawstwo*, 16, 2022, 270.

⁷⁷ P. DE BEER, *Framed by Section 8: Constitutional Protection of Privacy in Canada*, in *Canadian Journal of Criminology and Criminal Justice*, 50(3), 2008, 279 ss.



sunta in nome della sicurezza nazionale, ma deve superare un test di proporzionalità e necessità sancito dalla *Section 1* della Carta⁷⁸.

Sebbene il Paese non riconosca un diritto costituzionale esplicito alla privacy come avviene negli Stati Uniti, le sezioni 7 e 8 della *Canadian Charter of Rights and Freedoms* (1982) contengono disposizioni analoghe al Quarto Emendamento statunitense⁷⁹.

«Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice» (art. 7).

«Everyone has the right to be secure against unreasonable search or seizure» (art. 8).

La *Canadian Charter of Rights and Freedoms* può essere considerata una consolidata “bill of rights”, in quanto riconosce diversi diritti e libertà civili fondamentali, analoghi a quelli della sua controparte americana, tra cui: (1) libertà di coscienza, pensiero, espressione e credo; (2) diritto di voto; (3) libertà di espressione; (4) libertà di stampa; e (5) diritto alla vita, alla libertà e alla sicurezza della persona.

Nel 1983, il Parlamento canadese approva il *Privacy Act* al fine di garantire ai cittadini canadesi un pieno diritto alla privacy. La legge disciplina le modalità con cui il governo può raccogliere, conservare e, infine, divulgare le informazioni personali dei cittadini. Essa stabilisce inoltre il diritto degli individui ad accedere ai dati detenuti dal governo federale e a richiederne la correzione qualora risultassero inesatti.

L'articolo 7 del *Privacy Act* stabilisce che i dati biometrici “saranno utilizzati solo per gli scopi per i quali sono stati raccolti, o per un utilizzo coerente con tale scopo”⁸⁰. Nonostante il sistema di sorveglianza delle frontiere risponda a criteri di legalità (sez. 7 e 8 della *Charter*), la critica si sposta sulla necessità dell'uso di dati biometrici massivi, dove il bilanciamento tra sicurezza e rimedi effettivi (come l'intervento del *Privacy Commissioner*) rappresenta la griglia di controllo democratica assente nel modello cinese.

5.1. La securitizzazione delle frontiere in Canada

Nello studio *Hands Across the Border*, il *Standing Committee on Citizenship and Immigration* degli Stati Uniti raccomandò l'adozione di nuove tecnologie e un rafforzamento della cooperazione tra le autorità statunitensi e canadesi. La *Smart Border Declaration* e il *30-Point Action Plan* rappresentano i principali risultati di tali iniziative. Quest'ultimo, reso pubblico il 9 settembre 2002, mirava a stabilire standard uniformi per l'impiego biometrico delle impronte digitali e della scansione dell'iride, prevedendo tecnologie “interoperabili e compatibili per la lettura di questi dati biometrici” ai valichi di frontiera tra Stati Uniti e Canada⁸¹. Tra le prime iniziative, il Canada si impegnò a lanciare il programma pilota *NEXUS-Air 2000* dedicato ai viaggiatori aerei e a introdurre una nuova carta *biometric-ready* per i residenti permanenti. Parallelamente, il programma *Advance Passenger Information/Passenger Name Record* (API/PNR) si è rivelato uno strumento utile per lo scambio di informazioni pre-viaggio nei database delle compagnie aeree,

⁷⁸ K. FINLAY, *The Canadian Clearview AI Investigation as a Call for Digital Policy Literacy*, in *Surveillance & Society*, 21(1), 2023, 1 ss.

⁷⁹ A. LEVIN, M.J. NICHOLSON, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, in *University of Ottawa Law & Technology Journal*, 2, 2005, 378.

⁸⁰ T. SHEPHERD, *The Canadian Clearview AI Investigation as a Call for Digital Policy Literacy*, in *Surveillance & Society*, 21, 1, 2023, 1 ss. Disponibile a: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/16300/> (ultimo accesso 14 novembre 2024).

⁸¹ E. ZUREIK, K. HINDLE, *Governance, Security and Technology: The Case of Biometrics*, in *Studies in Political Economy*, 73(1), 2004, 125.

con particolare attenzione ai cosiddetti “visitatori ad alto rischio”⁸². I dati API/PNR possono potenzialmente rivelare possibili comportamenti criminali, tra cui terrorismo o crimini ad esso connessi, traffico di droga, tratta di esseri umani e altri crimini internazionali rilevanti (CBSA)⁸³.

In particolare, dopo gli eventi dell’11 settembre, i sistemi di sorveglianza e controllo aeroportuale hanno assunto una connotazione marcatamente selettiva sul piano etnico-religioso, traducendosi in pratiche di profilazione che hanno gravato in misura sproporzionata sui viaggiatori di fede o appartenenza musulmana. A tale riguardo, risulta illuminante il contributo teorico di Ghassan Hage, il quale, attraverso il concetto di *anxiety of stasis*, traducibile come “ansia dell’impasse”, ha messo in luce una forma di confinamento esistenziale e spaziale che colpisce in modo elettivo le comunità musulmane. Tale condizione non si esaurisce nella dimensione fisica della restrizione al movimento, ma investe la sfera identitaria e psicologica dell’individuo, il quale si trova sottoposto ad una costante condizione di vulnerabilità⁸⁴.

Questo fenomeno richiama il concetto di *social sorting* introdotto da David Lyon, secondo cui gli individui vengono classificati sulla base di criteri diversi per determinare chi debba ricevere maggiore attenzione, sospetto, inclusione, idoneità o accesso⁸⁵. In tale contesto, la tecnologia apparentemente neutrale, se applicata in un ambiente socialmente stratificato, tende inevitabilmente ad amplificare e consolidare tali disuguaglianze⁸⁶.

Sulla scia degli attentati dell’11 settembre 2001, lo spazio aeroportuale ha assunto una nuova dimensione di controllo e sorveglianza, in cui le pratiche di sicurezza si sono progressivamente orientate verso forme di profilazione etnico-religiosa. I viaggiatori di fede o apparenza musulmana si sono trovati esposti a scrutini sistematici fondati non sulla condotta individuale, bensì sull’identificazione di caratteristiche esteriori e indicatori corporei associati all’identità musulmana, dando luogo a prassi di screening selettivo che hanno sollevato rilevanti questioni in materia di non discriminazione e tutela dei diritti fondamentali.⁸⁷

Nel suo rapporto al Parlamento per il 2001–2002, il *Privacy Commissioner* of Canada, George Radwanski, criticò duramente le misure adottate nel post-11 settembre, evidenziandone il possibile impatto sui diritti alla privacy e alla sicurezza dei cittadini canadesi. Radwanski osservò che, con il pretesto dell’antiterrorismo, il diritto umano fondamentale alla privacy rischia di essere violato in Canada come mai prima, e il paese potrebbe avviarsi verso la perdita irreversibile sia di elementi chiave del sistema canadese di libertà, sia dei diritti alla privacy fino ad allora considerati acquisiti⁸⁸.

Piuttosto che sacrificare le libertà individuali e collettive in nome della securitizzazione, Radwanski propose alcuni criteri che ogni nuova legislazione “di sicurezza” dovrebbe rispettare prima della sua attuazione: la legge deve essere necessaria, dimostrare efficacia nel raggiungimento dello scopo, essere pro-

⁸² *Ibid.*

⁸³ Canada Border Services Agency, *Scenario Based Targeting*, 12 dicembre 2024. Disponibile a: <https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-airp/sbt-cfs-eng.html> (ultimo accesso 12 dicembre 2024).

⁸⁴ C. GIDARIS, *Rethinking Confinement through Canada’s Alternatives to Detention Program*, in *Incarceration*, 1(1), 2020.

⁸⁵ D. LYON, *Surveillance and Social Sorting: Privacy, Risk and Digital Discrimination*, cit., 2003, 37-38.

⁸⁶ S. LEMAN-LANGLOIS, *Big Data Against Terrorism*, in D. LYON, D. MURAKAMI WOOD (a cura di), *Big Data Surveillance and Security Intelligence: The Canadian Case*, Vancouver, 2021, 57 ss., 62.

⁸⁷ *Ivi*, 78.

⁸⁸ E. ZUREIK, K. HINDLE, *op. cit.*, 80.



porzionata alla minaccia e, infine, risultare dimostrabile che nessuna misura meno invasiva per la privacy sarebbe altrettanto efficace⁸⁹.

Tre episodi relativi a violazioni dei diritti alla privacy risultano particolarmente emblematici. Nel 2002, Maher Arar, cittadino siriano-canadese, fu detenuto al JFK International Airport e rimpatriato in Siria, dove venne torturato, a causa dell'inclusione erronea del suo nome in una "lista di controllo" di presunti terroristi. In un caso analogo, Alistair Butt, uno studente innocente di Orleans (Ontario, Canada), fu inserito per errore in una nuova *lista no-fly* istituita dal governo canadese in conformità con le normative statunitensi sulla sicurezza (*Passenger Protect Programme*); da allora, ogni viaggio aereo lo costringe a dover dimostrare la propria innocenza⁹⁰.

Un terzo caso riguarda Berna Cruz, cittadina canadese trattenuta e interrogata all'O'Hare International Airport di Chicago il 26 gennaio 2003 dagli agenti del *US Immigration and Naturalisation Service* (INS), prima di essere "deportata" in India. Cruz stava effettuando un volo di collegamento da Chicago a Toronto al termine di un viaggio di tre settimane in India. All'arrivo a Chicago, un agente doganale statunitense fermò Cruz sostenendo che il suo passaporto canadese apparisse "strano" e contenesse sostanze chimiche non identificate. Durante l'interrogatorio, Cruz fu sottoposta a domande insolite, tra cui il motivo del suo nome latino e del fatto che il suo cognome non fosse Singh⁹¹.

Questi tre casi evidenziano situazioni in cui le violazioni della privacy informativa hanno avuto effetti negativi e dannosi sulla vita delle persone e delle loro famiglie⁹².

Per contrastare il terrorismo aereo, nel 2007 il Canada ha istituito il *Passenger Protect Programme* (PPP), una reincarnazione della *No Fly List* statunitense, con l'obiettivo di impedire a terroristi noti o "potenziali" di imbarcarsi sugli aerei, identificando i rischi rappresentati dai viaggiatori attraverso l'analisi dei dati personali mediante algoritmi informatici⁹³.

Tuttavia, Faisal Bhabba, consulente legale e presidente del *National Council of Canadian Muslims*, ha denunciato il PPP come "uno degli strumenti più dannosi di profilazione razziale e religiosa", caratterizzato da pregiudizi istituzionalizzati che colpiscono ingiustamente e in modo sproporzionato i musulmani canadesi⁹⁴. A conferma di ciò, il PPP ha designato erroneamente centinaia di bambini canadesi – molti dei quali musulmani – come minacce ad alto rischio per la sicurezza dei trasporti. Tra questi figurano Sebastian Khan, di sei anni, Naseer Muhammad Ali, di undici anni, e Syed Adam Ahmed, di sei anni, che hanno visto limitata la loro libertà di movimento senza alcuna giustificazione se non il loro nome di nascita, violando il diritto alla libertà di movimento sancito dall'art. 13 della *UDHR*.

Ne consegue che i valori fondamentali di dignità, integrità e autonomia – tutelati dagli articoli 7 e 8 della *Canadian Charter of Rights and Freedoms* – risultano direttamente compromessi da pratiche di raccolta biometrica non consensuale. A tale riguardo, la Corte Suprema del Canada ha chiaramente statuito che il corpo umano costituisce la manifestazione esteriore dell'identità personale, e che la raccolta non consensuale di informazioni corporee, integra un'intrusione grave nella sfera più intima dell'individuo, ledendo

⁸⁹ *Ivi*, 81.

⁹⁰ L.R. SHADE, *Reconsidering the Right to Privacy in Canada*, in *Bulletin of Science, Technology & Society*, 28(1), 2008, 81.

⁹¹ S. BROWNE, *Digital epidermalization: Race, identity and biometrics*, in *Critical Sociology*, 36(1), 2010, 132.

⁹² L.R. SHADE, *Reconsidering the Right to Privacy in Canada*, cit., 81.

⁹³ C. GIDARIS, *op. cit.*, 84.

⁹⁴ *Ivi*, 86.

irreversibilmente i valori della Carta canadese⁹⁵. Tale condotta mina altresì la protezione dei diritti umani fondamentali, tra cui il diritto alla privacy (art. 12 UDHR), il diritto di lasciare il proprio paese (art. 13 UDHR), il diritto di cercare asilo (art. 14 UDHR) e il diritto a non essere sottoposti ad arresto, detenzione o esilio arbitrari (art. 9 UDHR).

Il *Temporary Resident Biometrics Project* (TRBP) del 2013 rappresenta un programma basato su dati biometrici destinato ai viaggiatori in ingresso in Canada con visti di soggiorno temporaneo provenienti da specifici paesi selezionati. Il progetto richiede ai cittadini stranieri la fornitura di informazioni biometriche aggiuntive, come impronte digitali e rilevamento facciale, al fine di verificare l'identità dichiarata prima dell'arrivo. Tali dati vengono inoltre condivisi con altre agenzie federali, tra cui la *Canada Border Services Agency* (CBSA) e la *Royal Canadian Mounted Police* (RCMP)⁹⁶.

Oggi, i cittadini canadesi sono sensibilmente più attenti alla protezione della privacy rispetto al passato. A conferma di ciò, il *Canadian Privacy Commissioner* ha deciso nel 2021 di vietare l'uso di *Clearview AI*, un software statunitense e principale fornitore di tecnologie di riconoscimento facciale (FR) per le forze di polizia canadesi⁹⁷.

Clearview AI metteva a disposizione delle forze dell'ordine versioni di prova gratuite del proprio strumento di riconoscimento facciale, permettendo di raffrontare fotografie caricate sulla piattaforma con un database di circa tre miliardi di immagini facciali, acquisite senza il consenso degli interessati attraverso lo scraping sistematico di piattaforme di social media – tra cui Facebook e Instagram – e di numerosi altri siti web accessibili pubblicamente⁹⁸. Le pratiche adottate da *Clearview AI* hanno sollevato serie perplessità sotto il profilo della conformità normativa e della trasparenza. Da un lato, la società ha violato i termini di servizio di numerose piattaforme di social media, appropriandosi di immagini facciali per finalità di riconoscimento biometrico senza alcuna autorizzazione da parte né delle piattaforme stesse né degli utenti ritratti. Dall'altro, *Clearview AI* non ha mai reso pubblici né le specifiche operative del proprio software né i dati relativi all'accuratezza del sistema, disattendendo in tal modo i requisiti minimi di trasparenza che la correttezza nei confronti degli utenti e delle autorità di controllo avrebbe imposto⁹⁹. Di conseguenza, l'*Office of the Privacy Commissioner* (OPC) e la *Royal Canadian Mounted Police* (RCMP) hanno stabilito congiuntamente che l'uso di *Clearview* da parte della RCMP violava le leggi federali e provinciali sulla privacy. Ne è derivato il divieto assoluto di operare in Canada e l'obbligo per *Clearview* di distruggere tutti gli archivi biometrici e le immagini facciali dei cittadini canadesi in suo possesso¹⁰⁰.

⁹⁵ Y. STEVENS, S. SOLOMUN, *Facing the Realities of Facial Recognition Technology: Recommendations for Canada's Privacy Act*, in *Cybersecure Policy Exchange*, Toronto, 2021, 11.

⁹⁶ R. PERO, H. SMITH, *In the 'Service' of Migrants: The Temporary Resident Biometrics Project and the Economization of Migrant Labor in Canada*, in *Geographies of Migration*, 2018, 191-202.

⁹⁷ J. SARABDEEN, *Protection of the Rights of the Individual when Using Facial Recognition Technology*, in *Heliyon*, 8(3), 2022.

⁹⁸ *Ivi*, 6.

⁹⁹ M. MARTIN, T. OWEN (a cura di), *Routledge Handbook of Human Security*, Londra, 2013.

¹⁰⁰ Office of the Privacy Commissioner of Canada, *Audit of Canada Border Services Agency's Compliance with Privacy Requirements*, 2017. Disponibile a: https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_cbsa_2017/ (ultimo accesso 12 dicembre 2024).



5.2. Evoluzioni recenti tra immigrazione e regolamentazione

Nell'ottobre del 2024, il Ministro canadese per l'Immigrazione, i Rifugiati e la Cittadinanza ha presentato il Piano sui Livelli di Immigrazione 2025-2027, prevedendo una diminuzione dei flussi migratori¹⁰¹. Sorge spontaneo chiedersi: come la tecnologia influirà sui processi decisionali dei richiedenti asilo? Le ricerche evidenziano che, a partire dal 2014, i sistemi di immigrazione e asilo del Canada hanno integrato strumenti automatizzati di decisione, come *Advanced Data Analytics* e *Algorithmic Impact Assessment* (AIA), per migliorare efficienza e produttività¹⁰².

Nonostante l'impegno verso la neutralità, le tecnologie come l'IA suscitano preoccupazioni in quanto potrebbero produrre risultati fuorvianti o distorti, perpetuando discriminazioni e rinforzando le disuguaglianze preesistenti. Tuttavia, con l'adozione dell'*AI Act* da parte dell'Unione Europea nel maggio 2024, il Canada vede una possibile soluzione nell'istituzione di agenzie indipendenti che monitorino e valutino da vicino l'implementazione di tecnologie di IA. In questo quadro si inserisce la creazione, nel novembre 2024, del *Canadian Artificial Intelligence Safety Institute* (CAISI), con il quale il Canada ha inteso valorizzare il proprio ecosistema di ricerca sull'intelligenza artificiale e il patrimonio di competenze scientifiche nazionali. L'istituto ha il mandato di approfondire la comprensione dei rischi connessi ai sistemi di IA, elaborando al contempo strategie volte a massimizzarne i benefici sociali ed economici in modo sicuro e responsabile¹⁰³.

Il governo cinese sembra andare in direzione contraria rispetto ad altri Paesi per quanto riguarda la regolamentazione dell'IA. Infatti, lo scorso marzo, è stata presentata una bozza di legge denominata *Artificial Intelligence Law of the People's Republic of China (Draft for Suggestions from Scholars)*, in quanto elaborata da accademici. La proposta mira principalmente a sostenere lo sviluppo tecnologico dell'industria dell'IA in risposta alla competizione tra Stati Uniti e Cina, rispetto alla tutela dei diritti delle persone fisiche¹⁰⁴. Se approvata, la legge completerebbe le normative già esistenti in Cina, come quelle su deepfake e raccomandazioni algoritmiche: *Provisions on the Management of Algorithmic Recommendations in Internet Information Services* del dicembre 2021, the *Provisions on the Administration of Deep Synthesis Internet Information Services* del novembre 2022, e infine *Measures for the Management of Generative Artificial Intelligence Services* dell'aprile 2023.

Sebbene il testo si concentri sullo sviluppo industriale, prevede comunque che i fornitori rispettino le leggi vigenti sulla protezione dei dati personali. Ad esempio, non sarà consentito utilizzare l'IA per analizzare e valutare comportamenti, abitudini, interessi o informazioni economiche, sanitarie e creditizie degli indi-

¹⁰¹ Government of Canada, *Government of Canada reduces immigration*, 2024. Disponibile a: <https://www.canada.ca/en/immigration-refugees-citizenship/news/2024/10/government-of-canada-reduces-immigration.html> (ultimo accesso 12 dicembre 2024).

¹⁰² M. ROSHAN, *The Role of AI in Canadian Immigration Processing*. Toronto Metropolitan University, Centre for Immigration and Settlement, 10, 2024.

¹⁰³ Government of Canada, *Government of Canada reduces immigration*, cit.

¹⁰⁴ CSET, *Artificial Intelligence Law of the People's Republic of China (Draft for Suggestions from Scholars)*, 2024. Disponibile a: <https://cset.georgetown.edu/publication/china-ai-law-draft/> (ultimo accesso 12 dicembre 2024).

vidui. Tuttavia, il fulcro della proposta resta favorire lo sviluppo rapido dell'industria dell'IA, attraverso misure come incentivi fiscali, supporto politico e la formazione di talenti nelle università¹⁰⁵.

6. Unione Europea: *Artificial Intelligence Act (AI Act)* e il divieto di identificazione biometrica in tempo reale

In questo studio comparativo, l'*Artificial Intelligence Act (AI Act)* europeo, viene assunto come *tertium comparationis*. Sebbene l'analisi si concentri su Cina e Canada, il Regolamento UE rappresenta oggi la *best law* disponibile: un modello di riferimento che permette di valutare, per contrasto, quanto il modello cinese di discosti dagli standard di tutela democratica e quanto il quadro canadese necessiti di un aggiornamento legislativo per raggiungere un livello di protezione analoga. L'*AI Act* – il Regolamento volto a disciplinare l'intelligenza artificiale, attraverso un impianto normativo unitario, organico e coerente, destinato a valere sull'intero territorio dell'Unione – è entrato in vigore nell'Agosto 2025, esattamente un anno dopo dalla sua pubblicazione. Tale Regolamento adotta un approccio basato sul livello di rischio delle diverse applicazioni e punta a trovare un equilibrio tra le opportunità legate alla ricerca e allo sviluppo dell'AI e i potenziali rischi che alcune tecnologie comportano per i diritti fondamentali e la protezione dei dati personali¹⁰⁶. Il Regolamento non si limita a comprendere programmatori, produttori e fornitori stabiliti nell'Unione, ma si applica a qualsiasi sistema di IA immesso o utilizzato nell'UE, indipendentemente dal luogo in cui è stato sviluppato o fabbricato. Tale approccio è chiamato *The Brussels Effect*, ovvero «il potere unilaterale dell'UE di regolare i mercati globali»: i sistemi di IA sviluppati in paesi terzi – come gli USA o la Cina – potranno essere commercializzati o utilizzati nell'Unione soltanto se conformi al quadro normativo adottato a Bruxelles¹⁰⁷. Il Regolamento è fondato su quattro livelli di rischio, in base all'impatto dei sistemi AI sui diritti fondamentali, sulla sicurezza e tutela dei dati personali. In primo luogo, vengono individuali i sistemi proibiti, in quanto ritenuti capaci di generare rischi considerati inaccettabili (art. 5). Segue la categoria dei sistemi ad alto rischio, per i quali è necessario superare una procedura di valutazione di conformità che ne certifichi "l'affidabilità" e il rispetto di specifici requisiti tecnici (art. 6). Infine, i sistemi a rischio basso o minimo possono circolare liberamente nel mercato, fermo restando il rispetto di taluni obblighi di trasparenza (art. 52)¹⁰⁸.

Per quanto riguarda l'uso di sistemi di identificazione biometrica a distanza (RBI), l'*AI Act* opera una distinzione importante tra sistemi RBI in tempo reale (*real-time RBI*) e RBI posticipati (*post RBI systems*). I sistemi RBI in tempo reale implicano la cattura, il confronto e l'identificazione in diretta, mentre i sistemi RBI posticipati svolgono queste funzioni in maniera retrospettiva utilizzando dati raccolti precedentemente, come le registrazioni delle telecamere a circuito chiuso (CCTV). L'*AI Act* generalmente proibisce

¹⁰⁵ J. COSTIGAN, *China's New Draft AI Law Prioritizes Industry Development*, 2024. Disponibile a: <https://www.forbes.com/sites/johannacostigan/2024/03/22/chinas-new-draft-ai-law-prioritizes-industry-development/> (ultimo accesso 12 dicembre 2024).

¹⁰⁶ B. MARCHETTI, L. PARONA, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*, in *DPCE Online*, 1, 2022, 246.

¹⁰⁷ *Ibid.*

¹⁰⁸ *Ibid.*



l'uso dei sistemi RBI in tempo reale, secondo l'Articolo 5(1)(h)¹⁰⁹. La proibizione si applica quando tutte le seguenti condizioni sono soddisfatte: il sistema di IA deve essere un sistema RBI; l'attività svolta deve coinvolgere l'uso di tale sistema; l'uso deve avvenire in tempo reale; l'uso deve avere luogo in spazi aperti e accessibili al pubblico; l'uso deve essere a scopo di applicazione della legge¹¹⁰.

L'Articolo 5(1)(h) prevede alcune eccezioni significative. Lo stesso articolo consente l'uso di tale tecnologia se strettamente necessaria ai seguenti scopi: (i) la ricerca mirata di vittime di crimini specifici (ad esempio, tratta di esseri umani); (ii) la prevenzione di una minaccia alla vita o all'incolumità fisica delle persone, o la minaccia di un attacco terroristico; (iii) la localizzazione o identificazione di una persona sospettata di aver commesso un reato, quando necessario per l'indagine, la persecuzione o l'esecuzione di una pena, a condizione che il reato sia (a) indicato nell'Allegato II, e (b) sia punibile ai sensi della legge nazionale con una pena massima di almeno 4 anni¹¹¹. Invece, i sistemi RBI posticipati sono classificati come sistemi di intelligenza artificiale ad alto rischio, ai sensi dell'Allegato III. Ciò significa che tale proibizione presenta rischi più elevati per i diritti fondamentali degli individui¹¹². L'articolo 6, insieme all'allegato III, elenca i sistemi considerati ad alto rischio e ne specifica i relativi ambiti di applicazione. Rientrano in questa categoria: i sistemi di identificazione biometrica consentiti, quelli impiegati come componenti nelle infrastrutture critiche, i sistemi destinati ai processi di reclutamento, selezione, promozione e gestione del personale, quelli impiegati nell'erogazione del credito o dei servizi pubblici, nel settore sanitario, nelle attività delle forze di polizia, nell'amministrazione della giustizia, nei processi democratici e nelle procedure legate all'immigrazione¹¹³.

7. Osservazioni conclusive

A questo punto, è possibile rispondere alle domande iniziali:

RQ1: La sorveglianza biometrica ha un impatto sui diritti umani fondamentali?

RQ2: In che misura le tecnologie biometriche stanno influenzando i diritti umani fondamentali in Cina e in Canada?

Nonostante l'adozione di numerose normative, sia a livello internazionale che nazionale, è evidente che le tecnologie biometriche di sorveglianza abbiano avuto e continuino ad avere un impatto fortemente negativo sui diritti umani fondamentali, sia in Cina sia in Canada, seppur con differenze significative. In primo luogo, è essenziale considerare le condizioni di partenza: il Canada è una democrazia consolidata, mentre la Cina non lo è. In Canada, diritti come la privacy, la libertà di riunione e associazione, la libertà di religione e credo, la libertà di opinione ed espressione e la libertà di movimento sono tutelati. Al contrario, in Cina questi diritti sono sistematicamente violati, in particolare nei confronti di manifestanti, cittadini comuni e gruppi emarginati e perseguitati, incluse minoranze etniche e religiose, e ciò avveniva già

¹⁰⁹ A. GIANNINI, S. TAS, *AI Act and the Prohibition of Real-Time Biometric Identification: Much Ado about Nothing?*, in *Verfassungsblog*, 10 dicembre 2024, disponibile a: <https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/> (ultimo accesso: 14 novembre 2024).

¹¹⁰ H. ILAND, F. SCHETS, *AI Act explained: ban on real-time remote biometric identification in public spaces*, (2025).

¹¹¹ L'Allegato II dell'AIA contiene un elenco esaustivo di 16 reati penali per i quali i sistemi RBI in tempo reale possono essere utilizzati.

¹¹² A. GIANNINI, S. TAS, *op. cit.*

¹¹³ *Ibid.*

prima dell'introduzione delle tecnologie di sorveglianza biometrica. Di conseguenza, in Cina queste tecnologie non solo amplificano le pratiche di controllo e monitoraggio, ma fungono anche da strumento per accelerare politiche di sorveglianza di massa, aggravando ulteriormente le violazioni dei diritti umani. Inoltre, nonostante numerose premesse a differenza del Canada la Repubblica Popolare Cinese non ha ratificato il Patto Internazionale sui Diritti Civili e Politici, che è stato solo firmato il 5 ottobre 1998. Il sistema giudiziario cinese non è indipendente e, allo stato attuale, lo Stato dispone di pochi strumenti legali per regolamentare l'uso delle tecnologie biometriche. Ciò rende improbabile anche un'evoluzione giurisprudenziale che possa limitare o controllare l'impiego di queste tecnologie in modo da salvaguardare i diritti umani fondamentali.

Per quanto riguarda il Canada, invece, questo Paese ha ratificato il Patto, dispone di un sistema giudiziario indipendente e la sua Costituzione garantisce diritti fondamentali come la libertà di opinione ed espressione. Di conseguenza, l'opinione pubblica e la società civile hanno la possibilità di influenzare le normative sulla privacy. Un esempio recente di questa dinamica è la consultazione pubblica avviata nel giugno 2021 per raccogliere feedback su una bozza di linee guida e su un possibile quadro legislativo e politico per regolamentare l'uso delle tecnologie da parte della polizia. Le consultazioni hanno coinvolto partecipanti della società civile, del mondo accademico, delle forze dell'ordine, del sistema legale, delle imprese e di altri settori, oltre ad incontri con gruppi marginalizzati e organizzazioni per i diritti umani. Inoltre, negli ultimi venti anni, numerose iniziative hanno sensibilizzato l'opinione pubblica riguardo alla sorveglianza governativa¹¹⁴.

A suo discapito, dopo gli attentati dell'11 settembre, il Canada, seguendo l'esempio degli Stati Uniti, ha adottato nuove politiche di controllo delle frontiere. Queste politiche includono metodi preventivi che mirano a determinati gruppi attraverso lo screening di sorveglianza. Questo processo di "classificazione sociale" evidenzia come il confine stia diventando sempre più un elemento biopolitico, gestendo le persone come entità biologiche anziché come soggetti giuridici, con l'obiettivo di identificare e neutralizzare la "minaccia esterna". La volontà di adottare un approccio preventivo alla sicurezza è un elemento che accomuna sia i Paesi democratici che quelli autoritari, richiamando il concetto di "Ban-option" sviluppato da Didier Bigo¹¹⁵. Secondo questa visione, l'obiettivo finale non è tanto reprimere comportamenti devianti, quanto mantenere uno stato permanente di "eccezione" schmittiana, in cui le norme ordinarie sono sospese in favore di misure straordinarie per la gestione del rischio e della sicurezza. Sebbene entrambi i Paesi usino la biometria per la sicurezza, solo il Canada mantiene un sistema di garanzie procedurali e rimedi effettivi che tentano di rispettare il principio di proporzionalità, mentre in Cina la sorveglianza è un'estensione della sovranità statale che nega l'inderogabilità dei diritti civili.

Vale la pena esplicitare ciò che comparazione ha reso possibile scoprire e che due analisi nazionali separate non avrebbero potuto rivelare con la medesima forza argomentativa. Non è la tecnologia biometrica in sé a produrre violazione dei diritti fondamentali, ma il modello istituzionale e costituzionale in cui essa

¹¹⁴ Per citare alcuni esempi, la campagna "Stop Illegal Spying", lanciata nel 2013 dalla *British Columbia Civil Liberties Association* (BCCCLA), ha portato a una causa contro il *Communications Security Establishment* (CSE); la campagna "Stop Online Spying" del 2011, avviata da *OpenMedia*, si opponeva alle leggi di accesso legale; infine, l'*International Campaign Against Mass Surveillance* (ICAMS), avviata nel 2004, ha rappresentato un movimento internazionale per stabilire limiti globali alla sorveglianza di massa.

¹¹⁵ D. BIGO, *Security, Exception, Ban and Surveillance*, in D. LYON (a cura di), *Theorizing Surveillance: The Panopticon and Beyond*, 2006, 46.

si inserisce. Questo risultato non è ricavabile dall'analisi di un solo Paese: analizzare esclusivamente la Cina potrebbe far concludere che le tecnologie biometriche siano intrinsecamente oppressive; analizzare esclusivamente il Canada potrebbe indurre a ritenere che i sistemi democratici siano impermeabili agli abusi. La comparazione dimostra invece che la stessa tecnologia produce effetti radicalmente diversi a seconda della presenza o assenza di rimedi effettivi. In secondo luogo, la comparazione rivela una convergenza strutturale che sfugge analisi del singolo paese: entrambi i sistemi tendono, sotto la pressione della sicurezza, verso forme di *social sorting* e di profilazione preventiva che colpiscono in modo sproporzionato le minoranze etniche e religiose – gli Uiguri in Cina, i musulmani canadesi nel contesto post-11 settembre. La differenza non risiede nell'assenza di questa tendenza in Canada, ma nella presenza di meccanismi istituzionali capaci di nominarla, contrastarla e, in alcuni casi, correggerla. Infine, la comparazione consente di utilizzare l'*AI Act* europeo come strumento per misurare la distanza strutturale tra i due modelli: il Regolamento UE presuppone un sistema di *enforcement* indipendente e rimedi effettivi senza i quali il divieto di identificazione biometrica in tempo reale resterebbe lettera morta. Il Canada si avvicina a questo modello, pur necessitando di un aggiornamento legislativo; la Cina se ne allontana strutturalmente per assenza delle condizioni istituzionali che renderebbero quella normativa applicabile.

bio
law