La vulnerabilità del migrante nell'era delle *smart-borders* e delle tecnologie *lie-detecting*

Roberta Nobile*

THE VULNERABILITY OF THE MIGRANT IN THE AGE OF SMART-BORDERS AND LIE-DETECTING TECHNOLOGIES

ABSTRACT: At the borders, biometric recognition is being used to detect suspicious movements and anticipate the screening of migrants as they enter European borders. To this end, the EU has funded iBorderCtrl, an AI liedetecting system operated by a virtual border guard to interrogate travelers trying to cross borders by assessing facial microexpressions. Facial recognition raises serious concerns, among them the danger of surveillance and discriminatory profiling, which draw the edges of a group vulnerability. In addition, the creation of biometric records within the interoperability dimension contributes to exacerbating the vulnerability of the migrant.

KEYWORDS: Migrants; lie-detecting; biometrics; vulnerability; border control.

ABSTRACT: Alle frontiere il riconoscimento biometrico viene utilizzato per individuare movimenti sospetti e anticipare lo screening dei migranti che entrano nei confini europei. L'UE ha finanziato *iBorderCtrl*, un sistema di rilevamento delle menzogne gestito da una guardia di frontiera virtuale per interrogare i viaggiatori che cercano di attraversare le frontiere mediante la valutazione delle microespressioni facciali. Il riconoscimento facciale solleva preoccupazioni, tra cui il pericolo di sorveglianza e di profilazione discriminatoria, che disegnano i margini di una forma di vulnerabilità di gruppo. A questo si aggiunga la creazione di registri biometrici nella dimensione dell'interoperabilità, contribuendo ad aggravare la fragilità del migrante.

PAROLE CHIAVE: Migranti; lie-detecting; biometria; vulnerabilità; sorveglianza.

ISSN 2284-4503

* *Dottoranda di ricerca, Università Campus Bio-Medico di Roma. Mail: robertanobile110@gmail.com.* *Contributo sottoposto a doppio referaggio anonimo.*

1. Introduzione: il confine della paura o la paura del confine?

La digitalizzazione delle frontiere statali ha determinato la progressiva creazione delle frontiere intelligenti o *smart-borders*, che implementano i processi tecnologici di biometria, sorveglianza dei dati e automazione in tandem, all'interno di una esasperazione del binomio corpo-confine, decantato dalle tecnologie di *lie-detecting*, che condannano gli immigranti ad interrogazioni a cui rispondere con il corpo e non con la parola, assolvendo al ruolo di macchina della verità in veste di giudice del confine.

L'espansione della biometria nel controllo strategico militare dei flussi di persone è stata parallela alla sorveglianza biometrica delle frontiere volta a prevenire movimenti migratori indesiderati[1]. Diversi autori hanno posto in evidenza i cambiamenti indotti da nuove forme di sicurezza delle frontiere: Johnson ha osservato in che modo la militarizzazione dei confini, che va di pari passo con il crescente uso di tecnologie biometriche, abbia innescato una riarticolazione ed espansione della sovranità statale[2]. Per Longo «i confini zonali più ampi sono diventati frontiere, mentre ugualmente la sovranità assomiglia ad un imperium crescente», vale a dire un'autorità politica territorialmente illimitata[3]. Per Lyon il confine «ora è ovunque»[4].

Si parla, pertanto, di confini biometrici per descrivere il modo in cui la biometria riconfigura i margini della società e i corpi delle persone al suo interno. Studiando la sorveglianza dei dati nella guerra al terrore, è possibile mostrare come le tecniche biometriche implichino processi di oggettivazione, pratiche, cioè, che dividono e scompongono l'individuo in fattori di rischio calcolabili, trasformando, in tal modo, il soggetto in oggetto[5]. Tale oggettivizzazione si traduce in nuove tecnologie di sorveglianza che identificano "popolazioni sospette", "gruppi a rischio", separano i "cittadini" dagli "anti-cittadini" e dai "non-cittadini", disciplinano il corpo indisciplinato[6] riportandolo in una zona di calcolo e gestibilità e recuperandolo all'interno di intervalli normali di accettabilità. Le informazioni biometriche utilizzate per costruire i dati sono, inoltre, catturate dal vortice tecnologico turbinoso della *dataveillance*, ossia il processo silente e continuo di estrazione e analisi algoritmica dei dati degli individui[7]. L'obiettivo della *dataveillance* non è monitorare soggetti specifici[8], ma sorvegliare tutti per creare profili che possono

[1] L. Amoore, *Biometric borders: Governing mobilities in the war on terror*, in *Political Geography,* 25.3/2013, 336-351.
[2] C. Johnson, *et al., Interventions on the state of sovereignty at the border*, in *Political Geography,* 59/2017, 1-10.
[3] M. Longo, *The politics of borders: Sovereignty, security, and the citizen after 9/11*, Cambridge University Press, 2017.
[4] D. Lyon, *The border is everywhere: ID cards, surveillance and the other*, in *Global surveillance and policing*, 2013, 66-82.
[5] L. Amoore, *op.cit*., 340.
[6] C. Johnson, *op.cit*., 32.
[7] H. Pötzsch, *The Emergence of iBorder: Bordering Bodies, Networks, and Machines*, in *Environment and Planning D: Society and Space*, 33.1/2015.
[8] J. Van Dijck, *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, in *Surveillance & society,* 12.2/2014, 197-208; S. Degli Esposti, *When big data meets dataveillance: The hidden side of analytics*, in *Surveillance & Society,* 12.2/2014; L. Everuss, *AI, smart borders and migration*, in A. Elliott (a cura di), *The Routledge Social Science Handbook of AI*, London, 2021; B.O. Martins, M.G. Jumbert, *EU Border technologies and the co-production of security 'problems' and 'solutions'*, in *Journal of Ethnic and Migration Studies*, 2020.

essere impiegati per valutare la minaccia rappresentata dalle persone, determinando, consequenzialmente, uno spostamento delle pratiche di sorveglianza dall'esame mirato di popolazioni e di individui «alla terribile deriva del monitoraggio di massa[9]».
Il *rebordering* biometrico viene, pertanto, descritto come un esercizio di biopotere[10], mediante il quale i corpi stessi si trasformano in siti di molteplici codificazioni sociali che aprono o chiudono a possibilità e pratiche di *agency*[11].
All'interno di una progressiva depoliticizzazione dei confini, l'emersione di tecnologie di *lie-detecting*, di verdetti pronunciati da macchine biometriche della verità, contribuisce a tracciare confini invisibili e invalicabili, che disegnano e giudicano il volto del migrante, ancor prima condannato da una forma di vulnerabilità di gruppo e da una discriminazione identitaria, prigioniero di uno stigma etnico-sociale insormontabile.

2. Il progetto iBorderCtrl: il nuovo verdetto dei biomarcatori

Una delle principali caratteristiche che compongono il tessuto morfologico dei confini intelligenti è rappresentata dall'automazione, necessaria per utilizzare gli strumenti biometrici e condurre la sorveglianza dei dati, poiché la quantità di informazioni e i livelli di elaborazione richiesti per intraprendere tali processi richiedono forme di analisi guidate da algoritmi[12]. A tal riguardo, nell'ottobre 2018, l'UE aveva annunciato che stava finanziando un nuovo sistema automatizzato di controllo delle frontiere, chiamato *iBorderCtrl*, da sperimentare in Ungheria, Grecia e Lettonia. Il funzionamento di tale sistema si articola in due fasi. La prima fase prevede che al viaggiatore venga chiesto di fornire informazioni sulla sua persona e sui dettagli del viaggio. Queste indicazioni vengono, poi, verificate con vari database per determinare se sono soddisfatte le premesse per poter effettuare l'attraversamento di frontiera. Successivamente, al fine di accertare che le informazioni fornite dal viaggiatore siano corrette, la seconda fase del sistema *iBorderCtrl* prevede l'utilizzo di un sistema di *lie-detecting* di intelligenza artificiale gestito da una guardia di frontiera virtuale per interrogare i migranti che cercano di attraversare i confini, valutando al contempo i minimi dettagli delle loro espressioni facciali, note come microespressioni, utilizzando tecniche facciali e tecnologie di riconoscimento delle emozioni. La voce e il comportamento diventano più severi se il sistema sospetta che il soggetto stia mentendo. Infatti, l'avatar interagirà con il viaggiatore in modo autonomo, assurgendo al ruolo di giudice artificiale, decidendo, pertanto, quali domande porre, come comportarsi (ad esempio, può adattare il suo comportamento a quello dell'individuo interrogato, talvolta assumendo un atteggiamento piuttosto scettico se una risposta fornita sembra non essere corretta) e, infine, formulando la valutazione conclusiva riguardo il rischio complessivo derivante dal viaggiatore in base alle informazioni fornite nella fase iniziale e ai risultati del rilevamento dell'inganno, in modo da indirizzare, successivamente, il migrante

[9] D. LYON, *op. cit*., 10.
[10] L. AMOORE, *op. cit*., 345.
[11] G. KAFER, *Big Data Biopolitics*. in *Digital Culture & Society, 5*.1/2019, 23-42.
[12] B.A. RAJOUB, R. ZWIGGELAAR, *Thermal facial analysis for deception detection*, in *IEEE Transactions on Information Forensics and Security*, 9.6/2014; J.R. SIMPSON, *Functional MRI lie detection: Too good to be true?* in *The Journal of the American Academy of Psychiatry and the Law*, 36.4/2008; C. MOROSAN, *Information disclosure to biometric e-gates: the roles of perceived security, benefits, and emotions*, in *Journal of Travel Research, 57*.5/2018.

alle guardie di frontiera umane. Tale sistema si adatta a ciò che viene descritto come un «passaggio dei regimi di sicurezza da una modalità reattiva ad una modalità proattiva, collocata al centro delle logiche statali contemporanee incentrate sulla superiorità tecnologica e sulla sorveglianza persistente»[13].

A supportare *iBorderCtrl* vi è un sistema automatizzato di rilevamento dell'inganno chiamato *Automatic Deception Detection System* (ADDS), sviluppato presso la *Manchester Metropolitan University*, con l'obiettivo di classificare i dati biometrici in linea con microespressioni non verbali facciali, considerate biomarcatori di inganno[14], in grado, cioè, di agire come predittori della menzogna. I biomarcatori dell'inganno sono codificati come 38 caratteristiche, quali, ad esempio, battito di ciglia sinistro, aumento del rossore del viso o direzione del movimento della testa. Ciascuna caratteristica è estratta da un segmento video di un secondo in cui il migrante mente o meno nel momento in cui risponde ad una precisa domanda, anche se dalla documentazione disponibile, prodotta dal team di *iBorderCtrl*, non risulta essere chiaro come vengano generate le caratteristiche per il segmento. Il video viene acquisito a 30 fotogrammi al secondo con una risoluzione video di 640x480. Ogni modello di addestramento del dataset è costituito da un vettore di 38 caratteristiche e dall'etichetta che indica la verità o l'inganno. Per creare il set di dati, a 32 partecipanti viene assegnato un ruolo, con due soluzioni possibili, "veritiero" o "ingannevole", da svolgere durante l'intervista, nel corso della quale ogni partecipante dovrà rispondere a 13 domande e ogni risposta prodotta verrà successivamente segmentata in molti vettori. Il team di *iBorderCtrl* afferma che i biomarcatori dell'inganno sono segnali che assunti singolarmente non possono rivelare un comportamento ingannevole, ma che, invece, complessivamente possono essere utilizzati da un metodo ML per rilevare le bugie dei migranti. Ciò significa che, secondo tale modello, i comportamenti giudicati ingannevoli o veritieri costituiscono due categorie, non sovrapposte, che rappresentano un insieme di stati emotivi. Nell'assegnare un'etichetta al segmento video relativo ad una risposta, l'ADDS, pertanto, considera solo tali due possibilità di categorizzazione escludendo, di conseguenza, ulteriori opzioni possibili, nonostante il modello presenti due parametri per filtrare i segmenti non significativi quando non sussiste una categoria definita e strutturata per essi. Sul solco di tali perplessità, il 5 novembre 2018, un deputato del Parlamento europeo, Patrick Breyer, aveva chiesto l'accesso ai documenti relativi all'autorizzazione del progetto *iBorderCtrl* e a quelli elaborati nel corso di tale progetto, detenuti dalla Commissione europea. Tale richiesta era stata rifiutata dall'agenzia europea responsabile di *iBorderCtrl*, l'*European Research Executive Agency* (REA), in quanto avrebbe compromesso gli interessi commerciali del consorzio, compresi i diritti di proprietà intellettuale, costringendo, pertanto, Breyer ad intentare una causa contro essa al fine di ottenere la pubblicazione di documenti riservati sulla giustificabilità etica e la legalità della tecnologia. Il Tribunale

[13] L. SUCHMAN, K. FOLLIS, J. WEBER, *Tracking and targeting: Sociotechnologies of (in) security*, in *SAGE Publications Sage CA: Los Angeles*, CA, 2017.

[14] J.W. CRAMPTON, *Platform biometrics*, in *Surveillance & Society,* 17(1/2), 2019, 54-62; J. SÁNCHEZ MONEDERO, L. DENCIK, *The politics of deceptive borders: biomarkers of deceit'and the case of iBorderCtrl*, in *Information, Communication & Society,* 25.3/2022, 413-430; L. DINGES, *et al*., *Exploring facial cues: automated deception detection using artificial intelligence*, in *Neural Computing and Applications*, 2024, 1-27; D. MINKIN, L.T. BRANDNER, *Borderline decisions? Lack of justification for automatic deception detection at EU borders*, in *TATuP-Journal for Technology Assessment in Theory and Practice,* 33.1/2024.

dell'Unione Europea aveva emesso la sentenza il 15 dicembre 2021[15], secondo la quale la decisione della REA doveva essere annullata, nella parte in cui questa aveva omesso di statuire sulla domanda del sig. Patrick Breyer di accesso ai documenti riguardanti l'autorizzazione del progetto *iBorderCtrl* e, in secondo luogo, nella parte in cui aveva rifiutato di concedere l'accesso completo ad ulteriori documenti, nella misura in cui tali documenti contenevano informazioni non coperte dall'eccezione prevista all'art. 4, paragrafo 2 del regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione. Non soddisfatto da questa decisione, il 25 febbraio 2022 Breyer aveva presentato ricorso[16] sostenendo che «l'interesse pubblico alla divulgazione prevalesse sugli interessi commerciali privati[17]», con la necessità di garantire accuratezza e trasparenza durante l'intero iter procedurale della ricerca. Nella successiva decisione del 7 settembre 2023, la CGUE aveva, innanzitutto, confermato la sentenza del Tribunale stabilendo che l'interesse pubblico, che riguardava, in realtà, un'eventuale futura applicazione di sistemi basati su tecniche sviluppate nell'ambito di tale progetto, era stato soddisfatto dalla diffusione dei risultati.

Inoltre, la circostanza che i partecipanti al progetto *iBorderCtrl* siano tenuti a rispettare i diritti fondamentali e i principi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione Europea, e che la Commissione sia tenuta a vigilare sul rispetto di detti diritti e di detti principi, non è in grado di far presumere l'assenza di una qualsiasi violazione di tali diritti e principi e di escludere l'esistenza di un interesse pubblico prevalente alla divulgazione dei documenti relativi a tale progetto, a causa del possibile impatto delle tecniche utilizzate sulla protezione dei diritti fondamentali.

Sorgono, infine, domande critiche in relazione al modo in cui i ricercatori abbiano cercato di validare l'ADDS prima di condurre i programmi pilota[18]. L'esperimento di validazione fornito dal team consisteva nel testare le prestazioni del classificatore ML che sarebbe stato incluso nell'ADDS. Ciò suggerisce, però, che non sia stato effettuato un test con nuovi individui (non visti) i cui dati avrebbero dovuto essere preventivamente acquisiti, elaborati e classificati dal modello ML, generando, di conseguenza, perplessità e dubbi sull'effettiva correttezza del test del modulo ADDS. Il dataset di addestramento non soddisfa, inoltre, le ipotesi della maggior parte degli algoritmi di apprendimento automatico, poiché i campioni ottenuti da ciascun partecipante sono correlati e, quindi, i modelli generati risultano essere molto vicini nello spazio delle caratteristiche e, allo stesso tempo, molto distanti dai vettori generati per altre persone. In altre parole, i dati nello spazio delle caratteristiche risultano molto scarsi, il che può produrre diversi problemi procedurali e strutturali[19].

Pertanto, alla luce di tali considerazioni, il sistema ADDS risulta essere stato addestrato e testato non solo su un numero piccolo di soggetti, ma per di più composto prevalentemente da maschi europei, la

[15] Case T-158/19, *Breyer v. REA*, ECLI:EU: T:2021:902.
[16] Case C-135/22P, *Breyer v. REA*, ECLI:EU:C:2022:640.
[17] Case C-135/22P, *Breyer v. REA*, ECLI:EU:C:2023:640, para. 104.
[18] L. Brandner, S. Hirsbrunner, *Algorithmic fairness in police investigative work. Ethical analysis of machine learning methods for facial recognition*, in *TATuP – Journal for Technology Assessment in Theory and Practice*, 32.1/2023, 24–29; A. Selbst, *Disparate impact in big data policing*, in *Georgia Law Review*, 52.1/2017.
[19] In statistica, questo fenomeno è noto come maledizione della dimensionalità ed è particolarmente rilevante quando la dimensione del campione è inferiore al numero di dimensioni dei dati. Si veda, al tal proposito, N. Altman, M. Krzywinski, *The curse(s) of dimensionality*, in *Nat Methods*, *15*.6/2018, 399-400.

cui conseguente sottorappresentazione di determinati gruppi, come le persone di colore o le donne, nei set di dati di addestramento dell'IA può condurre inevitabilmente a valutazioni inaffidabili riguardo gli individui appartenenti a tali gruppi e, consequenzialmente, a risultati distorti e discriminatori[20].
Oltre a tali perplessità di matrice empirica, emergono considerazioni critiche riguardo il fondamento teorico del sistema ADDS, in quanto privo di una base scientifica fondata e condivisa. Infatti, la critica epistemologica[21] evidenzia la mancanza di un consenso scientifico sull'ipotesi che le intenzioni ingannevoli possano essere dedotte dalle microespressioni, sottolineando, di conseguenza, come l'uso di sistemi di rilevamento dell'inganno non risulti giustificato a meno che non si raggiunga un riconoscimento scientifico fondato e condiviso sulle relative basi teoriche, in grado di fornire linee guida per una regolamentazione omogenea. Esistono, pertanto, disaccordi riguardo i molteplici aspetti e i diversi livelli di astrazione delle emozioni. In primo luogo, l'interpretazione delle microespressioni come indicatori di inganno non risulta essere conclusiva, poiché gli psicologi hanno formulato altre ipotesi similmente ragionevoli su ciò che le microespressioni potrebbero indicare[22], mettendo di conseguenza in discussione il fondamento del funzionamento dell'ADDS, in quanto, ad esempio, se le microespressioni non sono indicative di inganno ma di emozioni represse e soffocate nell'inconscio, il sistema non misurerà ciò che dovrebbe verificare. In secondo luogo, emerge un disaccordo psicologico sul fatto che l'analisi facciale possa fornire una lettura universale delle emozioni come stati fissi, sulla base del risultato di studi che hanno evidenziato come le espressioni emotive dipendono da fattori culturali e sociali[23], impedendo, pertanto, di giungere ad una classificazione appropriata ed omogenea delle emozioni e dei dati da associare.
Alla luce di tali considerazioni, *iBorderCtrl* costituisce sicuramente un prodotto dell'IA emozionale[24], dell'informatica affettiva, che trova espressione nel modo di affrontare l'emozione come qualcosa che può essere osservata attraverso ciò che può essere rilevato, misurato e ricordato, con il supporto e l'utilizzo di metodologie di rilevamento che classificano il comportamento facciale e corporeo. In particolare, si tratta di tecniche di rilevamento che hanno acquisito importanza in un contesto di *datafication*[25], che si esplica nella tendenza a trasformare sempre più aspetti dei fenomeni sociali e del

[20] J. Rothwell, *et al*., *Silent Talker. A new computer-based system for the analysis of facial cues to deception*, in *Applied Cognitive Psychology*, 20.6/2006; L.F. Barrett, *et al*., *Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements*, in *Psychological science in the public interest*, 20.1/2019.
[21] Si rinvia a L. Podoletz, *We have to talk about emotional AI and crime*, in *AI & Society,* 38.3/2023, 1067–1082; F. Bacchini, L. Lorusso, *Race, again. How face recognition technology reinforces racial discrimination*, in *Journal of Information, Communication and Ethics in Society*, 17.3/2019; P. Helm, T. Hagendorff, *Beyond the prediction paradigm. Challenges for AI in the struggle against organized crime*, in *Law and Contemporary Problems*, 84.3/2021.
[22] H. Elfenbein, N. Ambady, *On the universality and cultural specificity of emotion recognition. A meta-analysis*, in *Psychological Bulletin*, 128.2/2002.
[23] L. Feldman Barrett, *et al*., *Emotional expressions reconsidered. Challenges to inferring emotion from human facial movements*, in *Psychological Science in the Public Interest*, 20.1/2019; L. Zhang, O. Arandjelović, *Review of automatic microexpression recognition in the past decade*, in *Machine Learning and Knowledge Extraction*, 3.2/2021.
[24] A. McStay, *Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy*, in *Big Data & Society,* 7.1/2020; T. Gremsl, E. Hödl, *Emotional AI: Legal and ethical challenges*, in *Information Polity,* 27.2/2022.
[25] C. Southerton, *Datafication*, in L.A. Schintler, C.L. McNeely (a cura di), *Encyclopedia of Big Data*, Cham, 2022.

ISSN 2284-4503

comportamento umano in formati quantificati che possono essere tabulati e analizzati. Infatti, nel sintetizzare non solo l'ideologia del "dataismo"[26], basata sulla spinosa relazione tra persone e dati, in particolare sul dominio e la supremazia dei dati sulla fragilità della dimensione umana, ma anche il simultaneo vuoto scientifico dei sistemi di riconoscimento affettivo e la cancellazione dei dubbi negli algoritmi di apprendimento automatico, *iBorderCtrl* emerge come un modello per la politica di governance basata sui dati, la manifestazione della tendenza al tecnosoluzionismo[27], una recente propensione che ha visto sia i governi che le aziende tecnologiche ricorrere a soluzioni tecnologiche, digitali, high-tech per diversi ordini di problemi, dai cambiamenti climatici alla carestia fino alla migrazione.

3. Il corpo come "doppio di dati" nel paradigma della vulnerabilità di gruppo

La crescente combinazione e integrazione delle pratiche e delle tecnologie di sorveglianza in un insieme ampio di dati e di informazioni dà luogo ad una forma di assemblaggio di sorveglianza[28], retta da muri invisibili di intelligenza artificiale che sfidano il confine corporeo. Designano, in tal modo, la convergenza di quelli che prima erano sistemi di sorveglianza discreti verso un punto in cui operano come un insieme turbinoso e offuscato, dai margini labili e incerti. Questa convergenza corrisponde all'obiettivo costante delle autorità di polizia di integrare i diversi sistemi informatici e banche dati per realizzare una forma di interoperabilità, basata sulla consultazione, sullo scambio e sulla condivisione ad ampio spettro dei dati, in grado di condurre progressivamente ad una smaterializzazione del corpo e alla costituzione di un "*doppio di dati*"[29]. L'assemblaggio della sorveglianza delle tecnologie di *lie-detecting* opera, infatti, astraendo i corpi umani dal loro contesto territoriale e scomponendoli in una serie di flussi discreti, che verranno, poi, riassemblati in "doppi di dati" con la possibilità, a loro volta, di essere sottoposti a forme di controllo e intervento.

Il corpo viene così scomposto, astratto e riassemblato attraverso i flussi di informazione: il risultato è un corpo disincarnato[30], un doppio informatico di pura virtualità, in cui l'interesse non risiede nei corpi completi ma nei frammenti di informazione che essi emanano. Questo nuovo modo di divenire trascende la corporeità umana e riduce la carne a pura informazione, producendo la moltiplicazione dell'individuo, la costituzione di un "sé" aggiuntivo[31]. Al di là della violenza implicita nella decomposizione e nella riscrittura del corpo in forma digitale, la sfida si traduce nel tentativo di reincarnare l'individuo[32] e di ripristinare la materialità fisica che è alla base e nelle conseguenze di queste reti informatiche. Come mantenere la distinzione tra il corpo e l'informazione su di esso quando il corpo stesso è costituito da informazioni: dov'è esattamente il passaggio tra la materia e l'informazione del corpo?

[26] J. VAN DIJCK, *op. cit*., 206.
[27] Cfr. D. ANDLER, *Il duplice enigma. Intelligenza artificiale e intelligenza umana*, Torino, 2024.
[28] Sul punto si rinvia: P. MOLNAR, *Technology on the margins: AI and global migration management from a human rights perspective*, in *Cambridge International Law Journal, 8*.2/2019, 305-330; G. KAFER, *Big Data Biopolitics*, in *Digital Culture & Society, 5*.1/2019, 23-42; E.L. HSU, *The sociological significance of non-human sleep*, in *Sociology, 51*.4/2017, 865-879.
[29] C. EPSTEIN, *Guilty bodies, productive bodies, destructive bodies: Crossing the biometric borders*, in *International Political Sociology* 1.2/2007, 149-164; B. AJANA, *Biometric citizenship*, in *Citizenship Studies* 16.7/2012, 851-870.
[30] K. Hill, *La tua faccia ci appartiene*, Milano 2024.
[31] *Ivi*, 40.
[32] *Ivi*, 42.

Come vengono definiti i confini del corpo? La distinzione stessa non è più evidente, ma diventa sempre più ambigua: cosa riguarda il corpo e cosa è l'informazione sul corpo?

Alla luce di tali considerazioni, le tecnologie di *lie-detecting* possono essere interpretate come una macchina panottica che effettua esperimenti sul corpo umano, riflettendo la crescente enfasi posta non solo sulla politicizzazione ma anche sull'informatizzazione della vita, attraverso la delineazione di dispositivi di sicurezza che presuppongono l'incertezza delle minacce, impiegando metodi radicali che diventano pratica legale e governando il «radicalmente sconosciuto»[33]. Inoltre, attraverso tali processi, «il futuro guadagna ingiustamente il primato sia sul presente che sul passato»[34], innescando comportamenti che si basano su meri stimoli e risposte senza una riflessione autocosciente. Questa capacità foucaultiana di creare vita e lasciare morire è utile a coloro che detengono il potere e ha, di conseguenza, importanti implicazioni per la vita di gruppi emarginati, come migranti e rifugiati. Tale discorso anti-stranieri profila le minoranze come sgradite, consentendo alla sorveglianza di proteggere la maggioranza da «rischi oscuri e informi»[35]. La giustificazione delle strategie di sorveglianza in nome della sicurezza interna appare come una carta vincente discorsiva che prevale su tutte le altre affermazioni e disposta a sacrificare la vulnerabilità di gruppi discriminati. Avanza progressivamente l'orizzonte del realismo della sorveglianza, l'idea secondo cui nonostante si riconoscano e si temano gli errori di un sistema, che limita le libertà e invade i diritti, non sia possibile ormai immaginare una società senza un controllo onnipresente. In tal modo, il discorso di *iBorderCtrl* rivela una tendenza a ritrarre le forze di polizia digitali impegnate nella prevenzione del crimine e nell'immobilizzazione dei sospetti come qualcosa di neutrale, naturalmente buona, che sembra richiamare l'immagine foucaultiana di un potere sorvegliato «attraverso una figura gerarchica continua che assicura l'obbedienza, comandata da buoni ufficiali e uomini di sostanza[36]». Emerge, sullo sfondo, la cristallizzazione del biopotere, della capacità di far vivere e lasciar morire, dove la biopolitica trae la sua conoscenza dalle disabilità biologiche e il binomio potere e conoscenza condensa la sua azione di intervento.

Alla luce di tali considerazioni, le tecnologie di *lie-detecting* contribuiscono ad evidenziare due volti della vulnerabilità del migrante: la *precariousness* e la *precarity*[37]. La prima identifica quella vulnerabilità che ogni essere umano condivide in ragione della sua condizione corporea, della sua finitezza e limitazione, dell'esposizione al bisogno e alla sofferenza, mentre la seconda dipende dalle forme sociali, politiche, economiche e relazionali che qualificano le vite dei singoli soggetti. Essendo l'ontologia dell'umano costitutivamente relazionale e sociale e poiché l'essere non è mai definitivamente scindibile dall'altro[38], nonché dalle norme sociali o dalle strutture politiche e sociali e storicamente date, il volto della vulnerabilità ontologica del migrante (*precariousness)* si dispiega nelle forme della sua distribuzione differenziale, sociale, ed economica (*precarity*). È l'oppressione sistemica e non occasionale, perpetrata ai danni di un gruppo, quale quello legato allo status di migrante, che crea una forma

[33] R. WICHUM, *Security as Dispositif: Michel Foucault in the Field of Security*, in *Foucault Studies,* 15/2013, 164-171.
[34] *Ibidem*.
[35] Z. BAUMAN, D. LYON, *Liquid Surveillance. A Conversation*, Cambridge, 2013.
[36] M. FOUCALT, *Sorvegliare e punire*, Torino, 1976.
[37] F. MACIOCE, *La vulnerabilità di gruppo*, Torino, 2021.
[38] *Ivi*, 25.

di identità di gruppo[39]; allo stesso modo, quando la vulnerabilità non è meramente individuale, ma dipende dal funzionamento di strutture di conoscenza e di potere, o da sistemi di distribuzione di risorse, si creano condizioni accresciute di debolezza ai danni di quelli che vengono percepiti come gruppi di individui, determinando, di conseguenza, una definizione conclusiva di "vulnerabilità di gruppo", senza che questo implichi l'assunzione di una prospettiva essenzialista. La dimensione di gruppo in questo senso non è ontologica, ma, almeno in una certa misura, è identitaria: sta nel trovarsi esposti, insieme ad altri, a medesime forme di oppressione in quanto si viene percepiti come parte di un gruppo[40]. L'oppressione non sta nella vittimizzazione diretta che si ha nel singolo caso, ma nella consapevolezza di tutti gli appartenenti al gruppo di essere esposti a questo rischio proprio in ragione di un'appartenenza identitaria che è collettiva. In un secondo senso, si può parlare di gruppo vulnerabile quando la vulnerabilità dipende da un analogo posizionamento di più individui all'interno di un determinato contesto, tale da condizionarne le possibilità d'azione, e tale, soprattutto, da influire sulla loro capacità di far fronte a rischi e incertezze e gestirne le conseguenze. Questo posizionamento, tuttavia, non ha alcun carattere identitario, cioè non può né essere rivendicato come tale dall'interno (in una sorte di *identity politics*), né può essere utilizzato dall'esterno in modo ascrittivo[41]. Le modalità assunte da tali dispositivi di *lie-detecting* contribuiscono a confinare i migranti all'interno del paradigma di una minoranza, non inferiore dal punto di vista numerico, ma costituito da un gruppo le cui possibilità di accesso al potere risultano limitate. L'identità di tale gruppo si riassume, pertanto, nella condizione di non *dominance*, di subalternità al potere, opaco e inspiegabile, della macchina della verità "intelligente", che costruisce il giudizio finale sulla base di dati estratti dal corpo: quale paura per quale volto?

4. I rischi delle banche dati nella dimensione di interoperabilità

Ad accentuare il profilo di debolezza e di vulnerabilità del migrante, all'interno della crescente e progressiva fluidità e disarticolazione del proprio corpo, quale nuovo strumento appetibile per le logiche di potere umano[42] e per le dinamiche al silicio, contribuisce la delicata e complessa gestione dell'utilizzo dei dati biometrici, associata alle ombre di una condivisione interattiva, che supera i margini nazionali e coinvolge una pluralità eterogenea di protagonisti.

I dati biometrici sono, infatti, considerati particolarmente sensibili in quanto consentono l'identificazione di un individuo attraverso la registrazione di caratteristiche personali immutabili[43]. La creazione di registri biometrici permanenti di rifugiati e migranti pone particolari preoccupazioni in materia di diritti umani. Nel caso dei rifugiati esiste il rischio, a causa delle insidie del *function creep*[44], che le loro informazioni possano essere condivise – intenzionalmente (ad esempio, come una forma di politica statale) o inavvertitamente (attraverso violazioni di dati/sistemi non sicuri) – con le autorità del Paese

[39] F. Macioce, *op.cit.*, 37.
[40] *Ibidem*
[41] L. Everuss, *op. cit.*, 35.
[42] N. Farahany, *Difendere il nostro cervello*, Milano, 2024.
[43] N. Farahany, *op. cit.,* 32.
[44] M. Tzanou, *The EU as an emerging 'Surveillance Society: The function creep case study and challenges to privacy and data protection*, in *ICL Journal*, 4.3/2010.

da cui sono fuggiti, aumentando le possibilità di ulteriori abusi e persecuzioni. In particolare, l'utilizzo di sistemi centralizzati per l'archiviazione delle informazioni biometriche può facilitare la sorveglianza e l'uso improprio delle informazioni e rendere, di conseguenza, più dannose le violazioni dei dati[45]. Nel 2018 erano emerse notizie sulla condivisione da parte del governo del Bangladesh dei dati biometrici dei rifugiati Rohingya raccolti dall'UNHCR con il Myanmar, il Paese da cui erano fuggiti dal terrore e dalle violenze. Tali notizie erano state confermate da Human Rights Watch, che aveva accusato l'UNHCR di aver fornito informazioni personali dei rifugiati al governo del Bangladesh. I dati biometrici, inizialmente raccolti ai fini della registrazione e dell'accesso ai servizi, erano stati condivisi per il rimpatrio in assenza di un consenso libero e informato da parte dei rifugiati, ponendoli, di conseguenza, inesorabilmente a rischio. Un fattore abilitante di tali collegamenti è la crescita dell'interoperabilità che supporta la condivisione dei dati tra organizzazioni umanitarie, governi nazionali e agenzie di sicurezza, allo scopo di creare una solida ed interattiva rete transnazionale di polizia[46].

A tal proposito, è utile sottolineare che dal 2018 la polizia italiana utilizza un sistema di riconoscimento facciale chiamato S.A.R.I.[47] per identificare, durante le indagini, un soggetto ignoto confrontando la foto del volto con quelle collezionate nella banca dati AFIS. Il sistema è in grado di fornire un elenco di immagini ordinato secondo un grado di similarità, i cui risultati vengono, poi, analizzati dagli operatori specializzati della Polizia scientifica. Il sistema SARI presenta due diversi moduli: *SARI Enterprise* e *SARI Real-Time*. Il primo modulo permette di individuare l'immagine di un sospettato, acquisita, ad esempio, dalle videocamere a circuito chiuso, e confrontarla con riproduzioni di volti presenti nelle banche dati in possesso della polizia. Il *SARI Real-Time*, invece, è in grado di analizzare in tempo reale i volti dei soggetti ripresi dalle telecamere installate in un determinato luogo e di confrontarli con una watch-list la cui grandezza è dell'ordine delle decine di migliaia di soggetti. *SARI Enterprise* è già utilizzato durante le indagini mentre SARI Real-Time, ancora non attivo, è pensato a supporto di operazioni di controllo del territorio in occasione di eventi e/o manifestazioni, sfruttando la sua peculiare potenzialità di generare degli *alert* quando nel video appaiono individui presenti nella *watch-list*. Dal punto di vista legale, la Polizia ha ricevuto l'approvazione dal Garante privacy per l'utilizzo di SARI Enterprise nel luglio 2018, riconoscendo che il sistema automatizza semplicemente un'attività che le forze di polizia hanno sempre svolto manualmente, ossia la ricerca dei volti per anagrafica e dettagli in AFIS[48]. Per *SARI Real-*

[45] Cfr. M. LATONERO, *et al*., *Digital identity in the migration and refugee context*, in *Data & Society,* 4/2019; R. THOMAS, *Biometrics, international migrants and human rights*, in *Eur. J. Migration & L.,* 7/2005; C. COSTELLO, I. MANN, *Border justice: migration and accountability for human rights violations,* in *German Law Journal,* 21.3/2020.

[46] Sul punto si rinvia a H. ADEN, *Interoperability between EU policing and migration databases: Risks for privacy*, in *European Public Law,* 26.1/2020; E. BROUWER, *Large-scale databases and interoperability in migration and border policies: The non-discriminatory approach of data protection*, in *European Public Law,* 26.1/2020; N. VAVOULA, *Interoperability of EU information systems: The deathblow to the rights to privacy and personal data protection of third-country nationals*, in *European public law,* 26.1/2020.

[47] R. LOPEZ, *La rappresentazione facciale tramite software*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2019; G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; E. SACCHETTO, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *La legislazione penale web*, 2020, 1-14.

[48] Garante per la protezione dei dati personali, Parere sul sistema Sari Enterprise, 26.7.2018, n. 440, doc. web n. 9040256, in www.garanteprivacy.it.

Time, invece, il Garante Privacy si era espresso nell'aprile 2021 definendo il sistema di riconoscimento facciale, così come progettato, una possibile forma di sorveglianza e identificazione di massa che non poteva essere utilizzata dal Ministero dell'Interno perché non vi era ancora una base legale per il trattamento di dati biometrici da parte delle forze dell'ordine[49].

Da un'analisi dei comunicati stampa delle Questure italiane emerge che il sistema SARI Enterprise è ampiamente utilizzato nelle attività di polizia e, in alcuni casi, le persone identificate sono cittadini stranieri presenti in Italia: tra i soggetti coinvolti vi sono persone di etnia rom, persone di origine algerina, e persone nate in Italia da genitori stranieri. Non sempre però la polizia spiega il motivo per cui l'immagine è già presente nel database AFIS, in alcuni casi è indicato che i soggetti coinvolti sono stati fotosegnalati in precedenza per aver commesso altri reati. I soggetti presenti in AFIS rientrano però anche in altre categorie. Infatti, secondo quanto previsto dal Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero (D.Lgs 286/1998), chi richiede il permesso di soggiorno o chi ne domanda il rinnovo è sottoposto a fotosegnalamento. Comprendere la composizione del database AFIS utilizzato con il sistema di riconoscimento facciale SARI è fondamentale per capire quali rischi corrono le persone che vi sono incluse. Il database AFIS è, infatti, utilizzato durante le indagini per cercare l'identità di un sospetto tra volti già noti alle autorità per aver commesso dei reati, includere nello stesso database migranti e richiedenti asilo rischia, di conseguenza, di criminalizzare ulteriormente tali soggetti. Secondo una recente inchiesta[50], 8 persone su 10 presenti nel database AFIS sarebbero stranieri, ovvero circa 2 milioni di cittadini italiani e 7 milioni di persone con cittadinanza diversa da quella italiana. Al momento in Italia vi è, quindi, il rischio che un richiedente asilo possa essere fermato e interrogato dalla polizia solo perché l'algoritmo del sistema SARI ha indicato un match con la foto di un soggetto schedato con il quale condivide solamente il colore della pelle. Alla luce di tali considerazioni, la composizione del database, la mancanza di informazioni e analisi sull'accuratezza degli algoritmi utilizzati e l'assenza di risposte precise da parte delle forze dell'ordine sollevano necessarie preoccupazioni sui rischi che il sistema SARI potrebbe produrre quando utilizzato su migranti e persone straniere presenti in Italia, soprattutto in luce delle novità introdotte dall'entrata in vigore dell'AI Act. Infatti, la recente legislazione sulla regolamentazione dell'intelligenza artificiale ha vietato la categorizzazione biometrica con lo scopo specifico di dedurre i dati sensibili e l'identificazione biometrica da remoto negli spazi pubblici, con alcune eccezioni riservate alle forze dell'ordine relative alla ricerca di criminali e vittime e alle minacce terroristiche[51], che potrebbero determinare, alla luce delle considerazioni sopra esposte, il riesame delle potenzialità di impiego del sistema *SARI in Real Time*. Nel contesto migratorio invece, pur affermando che i sistemi basati sull'IA non devono in alcun modo infrangere il principio di non-respingimento, l'AI Act si è limitato a inserire nella lista ad alto rischio[52] (senza proibirli) i poligrafi, la profilazione del rischio individuale, i sistemi per esaminare le richieste d'asilo e quelli per rilevare, riconoscere o identificare le

[49] Garante per la protezione dei dati personali, Parere sul sistema Sari Real Time, 25.3.2021, n. 127, doc. web n. 9575877, in www.garanteprivacy.it.

[50] Disponibile in www.asgi.it (ultima consultazione 03/07/24).

[51] Cfr. art. 5 dell'AI Act.

[52] Cfr. art. 6 dell'AI Act.

ISSN 2284-4503

persone ai confini[53]. Tuttavia, i legislatori dell'UE si sono rifiutati, almeno per il momento, di vietare sistemi dannosi come i sistemi di valutazione del rischio discriminatorio nella migrazione e l'analisi predittiva se utilizzata per facilitare i respingimenti. Inoltre, il divieto di riconoscimento delle emozioni non si applica al contesto migratorio, escludendo, pertanto, i casi documentati di macchine della verità IA alle frontiere. L'elenco dei sistemi ad alto rischio non tiene conto dei numerosi sistemi di IA utilizzati nel contesto della migrazione e che, di conseguenza, non risultano soggetti agli obblighi del presente regolamento. L'elenco esclude modelli pericolosi come i sistemi di identificazione biometrica, gli scanner di impronte digitali o gli strumenti di previsione utilizzati per prevedere, bloccare e limitare la migrazione. Sullo stesso fronte di lacune e incertezze, l'IA utilizzata in ausilio di banche dati su larga scala dell'UE in materia di migrazione, come Eurodac, il Sistema d'informazione Schengen e ETIAS, non dovrà essere conforme al regolamento fino al 2030, aprendo pericolosamente spazi di incertezze. La legge sull'IA non ha, poi, affrontato il modo in cui i sistemi di IA sviluppati da aziende con sede nell'UE possano avere un impatto sulle persone al di fuori dell'UE, nonostante le prove esistenti di violazioni dei diritti umani facilitate dalle tecnologie di sorveglianza sviluppate nell'UE e impiegate in Paesi terzi. Pertanto, allo stato attuale non sarà proibito esportare un sistema vietato in Europa al di fuori dei confini europei.

L'aspetto forse più dannoso della legge europea sull'IA è la creazione di un quadro giuridico parallelo quando l'IA viene impiegata dalle autorità di polizia, di immigrazione e di sicurezza nazionale. Grazie alle pressioni esercitate dagli Stati membri, dalle forze dell'ordine e dalle lobby dell'industria della sicurezza, queste autorità sono esplicitamente esentate dalle norme e dalle salvaguardie più importanti della legge sull'IA.

5. Conclusioni

Il progresso tecnologico ha contribuito ad accentuare i mille volti della vulnerabilità del migrante, rendendolo preda prelibata e cavia inconsapevole delle nuove sperimentazioni.

Gli Stati sono in grado di giustificare i crescenti esperimenti tecnologici in materia di migrazione perché i migranti sono stati storicamente considerati come una popolazione da gestire e quantificare. La stessa retorica della gestione della migrazione implica che i rifugiati e i migranti debbano essere sorvegliati e controllati, in quanto considerati una minaccia alla sovranità nazionale, soprattutto in tempi in cui sempre più gli Stati si rivolgono verso l'interno e reificano il loro potere. Il concetto di "esclusione inclusiva" di Agamben[54], in cui lo Stato è in grado di dividere e separare le popolazioni sulla base della figura del fuorilegge, che si trova al di fuori dei confini della vita sociale e politica dello Stato, rafforza ulteriormente il modo in cui immaginiamo che la differenziazione dei diritti sia naturale quando viene utilizzata per giustificare interventi e sperimentazioni ai margini per il cosiddetto bene comune. Il

[53] D. Ozkul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*. Oxford: Refugee Studies Centre, University of Oxford, 2023; J. Laux, S. Wachter, B. Mittelstadt, *Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk*, in *Regulation & Governance,* 18.1/2024; A. Mantelero, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, in *Computer Law & Security Review* 54, 2024.

[54] G. Agamben, *State of Exception*, University of Chicago Press, Chicago 2005.

ISSN 2284-4503

potere ultimo dello Stato di decidere chi può entrare e a quali condizioni è rafforzato dalla continua convinzione dell'imparzialità tecnologica, all'interno di una tensione intrinseca tra la prerogativa rivendicata dagli Stati nazionali sulla sovranità e la natura malleabile della tecnologia. Nella sua fluidità, la tecnologia è intrinsecamente contraria ai confini e, per estensione, alla sovranità, riverberando molto spesso i suoi effetti sulla definizione stessa di umanità nell'era digitale[55]. La distribuzione ineguale dei benefici che derivano dallo sviluppo tecnologico contribuisce a creare monopoli della conoscenza e a consolidare il potere e l'autorità conferiti allo Stato sovrano. Questi monopoli possono esistere perché non sussiste un regime normativo globale unificato che disciplini l'uso delle nuove tecnologie, creando laboratori per esperimenti ad alto rischio con un profondo impatto sulla vita delle persone più vulnerabili. Alla luce di tali considerazioni, le tecnologie di *lie-detecting* traducono l'immagine di un costrutto sociale, uno specchio in grado di riprodurre i problemi e i pregiudizi che sono già insiti nella società e che compromettono la pratica stessa della democrazia. L'interrogatorio biometrico prodotto dagli sviluppi dell'AI contribuisce a delineare un nuovo volto, una nuova figura, un corpo di cristallo del migrante, rotto in mille pezzi dal giudizio pronunciato da un avatar che si erge al ruolo di giudice naturalmente artificiale e che tenta di estrarre e tradurre i singoli cristalli in verdetti dell'intenzione, contribuendo ad aggiungere nuovi tasselli al mosaico della vulnerabilità: è la nuova frontiera per la nuova paura dell'artificiale? Un terrore al silicio?

[55] E. Zureik, K. Hindle, *Governance, Security and Technology: The Case of Biometrics*, in *Studies in Political Economy*, 2004.