ATTUALITÀ

BEATRICE ONOFRJ

Intelligenza artificiale e *crimmigration*: profili di discriminazione razziale del migrante alla luce del nuovo *AI Act* europeo

Il contributo esamina l'interazione tra intelligenza artificiale e fenomeno della *crimmigration,* con particolare riguardo ai profili di discriminazione etnico-razziale derivanti dall'impiego di tecnologie predittive e di riconoscimento facciale nei sistemi di controllo dei flussi migratori. L'analisi mette in luce come tali strumenti possano incidere sull'effettività delle garanzie individuali e amplificare *bias* strutturali già presenti nelle attuali politiche di sicurezza. In conclusione, viene valutato il contributo della legislazione europea e nazionale di settore nel delineare un quadro normativo idoneo a contemperare esigenze di efficienza amministrativa e tutela dei diritti fondamentali.

Artificial intelligence and crimmigration: racial discrimination against migrants in the context of the new European AI Act.

This paper explores the intersection between artificial intelligence and the phenomenon of crimmigrations, focusing on the ethnic and racial discrimination risks stemming from the use of predictive and facial recognition technologies in migration control systems. The analysis highlights how these tools may affect the effectiveness of individual safeguards and reinforce structural biases embedded in security policies. Finally, it assesses the contribution of both the European and the national legislation in shaping a regulatory framework capable of balancing administrative efficiency with the protection of fundamental rights.

1. *Premessa. L'automatizzazione come moltiplicatore di disparità già esistenti.*

L'avanzamento tecnologico e l'emergere dei cosiddetti sistemi di intelligenza artificiale[1] hanno catalizzato un fenomeno di portata rivoluzionaria che, pur

[1] Il termine venne coniato nel 1955 dal matematico John McCarthy, Professore presso il Darmouth College, nel documento contenente la proposta di ricerca per una conferenza tenutasi a Darmouth tra alcuni dei più importanti scienziati dell'epoca (cfr. MCCARTHY-MINSKY-ROCHESTER-SHANNON, *A proposal for the Darmouth Summer Research Project on Artificial Intelligence,* Hanover, 31 agosto 1955). La Carta Etica Europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, adottata dalla CEPEJ nel corso della sua 31ª Riunione plenaria (Strasburgo, 3-4 dicembre 2018) definisce l'intelligenza artificiale come «l'insieme di metodi scientifici, teorie e tecniche finalizzate

prospettando massimizzazione dell'efficienza e ottimizzazione funzionale, solleva con crescente urgenza la necessità di esaminare l'impatto che un impiego non adeguatamente regolamentato di tali tecnologie può avere sui diritti fondamentali degli individui coinvolti.

In ambito penalistico e processualpenalistico, ad esempio, ampia dottrina[2] ha da tempo segnalato le possibili distorsioni derivanti dall'impiego di sistemi automatizzati nel procedimento penale. In questo quadro, tra i profili maggiormente indagati assume rilievo quello concernente il rischio di effetti discriminatori[3] derivanti dall'utilizzo dell'IA nelle diverse fasi della gestione del feno-

---

a riprodurre mediante le macchine le capacità cognitive degli esseri umani.» (cfr. COMMISSIONE EUROPEA PER L'EFFICIENZA DELLA GIUSTIZIA, *Carta Etica Europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, app. III, Glossario, 47).

[2] Si vedano, tra gli altri, CARRATTA, *Decisione robotica e valori del processo penale*, in *Riv. dir. proc.*, 2020, 2, 491 ss.; CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in *www.sistemapenale.it,* 8 gennaio 2021; BACCARI-FELICIONI, *La decisione penale tra intelligenza emotiva ed intelligenza artificiale,* Padova, 2023; P. SEVERINO, *Intelligenza Artificiale e Diritto Penale*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di Ruffolo, Milano, 2020, 531 ss.; BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *Diritto Penale e Uomo*, 2019, 10, 1 ss.; UBERTIS, *Intelligenza artificiale e giustizia predittiva*, in *www.sistemapenale.it,* 16 ottobre 2023; *Decisione robotica,* a cura di Carleo, Bologna, 2019; PADUA, *Intelligenza artificiale e giudizio penale: scenari, limiti e prospettive*, in *Proc. pen. giust.*, 2021, 6, 1479 ss.; D'AGOSTINO, *Gli algoritmi predittivi per la commisurazione della pena. A proposito dell'esperienza statunitense nel c.c. evidence-based sentencing*, in *Dir. pen. cont.,* 2019, 2, 354 ss.; PRESSACCO, *Intelligenza artificiale e ragionamento probatorio nel processo penale,* in *Intelligenza artificiale e processo penale. Indagini, prove, giudizio,* a cura di Pressacco-Di Paolo, Napoli, 2022; IRTI-E. SEVERINO, *Dialoghi su diritto e tecnica*, Roma-Bari, 2001; GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *www.penalecontemporaneo.it,* 29 maggio 2019; QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion, Springer,* Alessandria, 2020; DI GIOVINE, *Il judge-Bot e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale),* in *Cass. pen.*, 2020, 951 ss.; MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *Intelligenza artificiale – Il diritto, i diritti, l'etica,* cit., 547 ss.; MASSARO, *Intelligenza artificiale e neuro-scienze: l'eterno ritorno del diritto penale?,* in *Derecho penal, inteligencia artificial y neurociencias*, a cura di Peris Riera-Massaro, Roma, 2023, 42 ss.; D'AMICO, *La misura della (im)prevedibilità. Modelli di imputazione della responsabilità ai tempi dell'intelligenza artificiale,* Napoli, 2025; FRAGASSO, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile",* Torino, 2025; PAULESU, *Intelligenza artificiale e giustizia penale. Una lettura attraverso i principi*, in *Arch. pen. web,* 9 maggio 2022; RICCIO, Ragionando su intelligenza artificiale e processo penale, in in *Arch. pen. web,* 21 novembre 2019; *Intelligenza Artificiale, Diritto, giustizia, economia ed etica*, a cura di Basile-Biasi-Camaldo-Caneschi, Fragasso-Milani, Torino, 2025.

[3] Sulla funzione "discriminante" delle tecnologie che si analizzeranno, occorre fare una precisazione: specialmente per quanto riguarda la legislazione sul controllo delle frontiere, naturalmente e funzionalmente ideata proprio per "discriminare" differenziando chi può entrare in un paese e chi no, si vuole indirizzare l'analisi sulla discriminazione «normativamente pregiudizievole», ovvero quella che differenzi il trattamento allocando risorse e tutelando i diritti fondamentali in modo differente sulla base di

meno criminale. Certamente, le disparità di matrice razziale in detto settore – particolarmente sentite in alcuni paesi, come negli Stati Uniti[4] – sono preesistenti[5] all'avvento dell'intelligenza artificiale, e affondano le loro radici in una pluralità di cause, la cui esaustiva individuazione e ricostruzione esula dagli obiettivi della presente analisi. Accanto ai determinanti di matrice storico-sociologica – quali l'eredità dei processi coloniali, le persistenti disuguaglianze socio-economiche e le politiche di controllo sociale che, storicamente, hanno esercitato un impatto sproporzionato sulle minoranze etniche – rileva altresì il ruolo dei *bias*[6] cognitivi che, sin da epoche risalenti e proprio a causa dei predetti fattori, influenzano l'operato degli attori istituzionali (in particolare, le forze di polizia[7], che nell'ambito dell'attività di prevenzione e repressione

caratteristiche etniche degli individui (Così TENDAY ACHIUME, *Symposium on undoing discriminatory borders. Digital racial borders,* in *Cambridge University Press*, 2021). Per discriminazione etnica o razziale – tipologia sulla quale si concentrerà il contributo – deve intendersi «qualsiasi forma di distinzione, esclusione, restrizione o preferenza che si basi sulla razza, il colore, la discendenza o l'origine nazionale o etnica, che abbia lo scopo o l'effetto di annullare o compromettere il riconoscimento, il godimento o l'esercizio, su base egualitaria, dei diritti umani e delle libertà fondamentali nel campo economico, politico, sociale, culturale o in qualsiasi altro campo della vita pubblica» (Definizione fornita dall'International Convention on the Elimination of All Forms of Racial Discrimination, Articolo 1).

[4] In Nordamerica il problema della c.d. *sentencing disparity* di origine razziale, intesa come variazione arbitraria nella commisurazione della pena e ritenuta sussistente dalla United States Sentencing Commission in un *Report* del 1991 quando «individui con simili precedenti penali, trovati colpevoli per fatti simili, ricevono pene diverse» (cfr. *The Federal Sentencing Guidelines: A Report on the Operation of the Guidelines System and Short-Term Impacts on Disparity in Sentencing, Use of Incarceration, and Prosecutorial Discretion and Plea Bargaining,* 1991), ha attanagliato la giustizia penale per decenni, rivelando ancora oggi uno dei lati più oscuri della gestione del fenomeno penale negli Stati Uniti (sul punto, per un'ampia disamina del problema e delle soluzioni ricercate dalla dottrina nordamericana, cfr. MANNOZZI, *Razionalità e giustizia nella commisurazione della pena. Il Just Desert Model e la riforma del sentencing nordamericano,* Padova, 1996, 242 ss.).

[5] Per uno studio sull'etnia delle persone decedute sotto la custodia della polizia nel Regno Unito v. ANGIOLINI, *Report of the independent review of deaths and serious incidents in police custody*, 2017, 83 ss., che sottolinea come la forte presenza di persone provenienti dalle comunità BAME (*Black, Asian and Minority Ethnic*) rifletta il razzismo sistemico presente nel paese. Un'altra ricerca, invece, condotta negli Stati Uniti negli anni '90, dimostrava come gli Afroamericani avessero una probabilità 4.85 volte superiore rispetto ai bianchi di essere fermati presso un posto di blocco su un'autostrada in New Jersey e ben 16.5 volte superiore di essere successivamente arrestati (v. LAMBERT, *Driving While Black. A statistician proves that prejudice still rules on the road*, in *The Washington Post*, 15 Agosto 1998).

[6] «Specifici errori di giudizio sistematici e prevedibili, prevalentemente di natura psicologica», così BLAIOTTA, *Giustizia, errore, intelligenza artificiale*, in *www.sistemapenale.it,* 23 ottobre 2023, 5.

[7] Sul punto, nel report stilato nel 1999 da Sir Ian Macpherson sulla morte di Stephen Lawrence in un passo in cui si cita la nota fornita dal Dr Robin Oakley all'inchiesta (*Institutional Racism and Police Service Delivery, Dr Robin Oakley's submission to this Inquiry*), si legge: «Il lavoro della polizia, a differenza di molte altre professioni, ha la capacità di mettere gli agenti in contatto con un segmento distorto della società, con il ben noto rischio di creare stereotipi negativi nei confronti di determinati gruppi.

tendono a ricercare la notizia di reato tra fasce sociali caratterizzate da indici di devianza più elevati[8], e gli organi giudicanti, nella funzione decisionale[9]). La discrezionalità della decisione autoritativa e/o giudiziale, spesso viziata da tali illusioni cognitive, ha quindi, nel tempo, portato alla creazione di disparità trattamentali tra soggetti appartenenti a etnie maggioritarie ed individui appartenenti a minoranze etniche (neri, nativi americani, messicani, nordafricani, nomadi, ecc.). Trattasi di un fenomeno certamente non limitato all'esperienza d'oltreoceano, ma dirompente anche ove si osservi il sistema penale e penitenziario del nostro Paese, ove, al 30 aprile 2025 i detenuti stranieri nelle carceri italiane per adulti erano 19.740, pari al 31,6%[10] del totale della popolazione detenuta, con molti istituti penitenziari dove i detenuti stranieri superano la metà del totale dei presenti[11], soprattutto nel nord del Paese e, purtroppo, negli Istituti penali minorili[12].

Orbene, l'introduzione di sistemi automatizzati e standardizzati a supporto dell'attività delle autorità titolari di poteri decisionali incidenti sui diritti fon-

---

Questi stereotipi diventano parte integrante della cultura professionale della polizia. Se il personale, per lo più bianco, dell'organizzazione ha la propria esperienza con le minoranze visibili limitata principalmente a interazioni con questi gruppi, è probabile che si sviluppino stereotipi razziali negativi». (MACPHERSON, *The Stephen Lawrence Inquiry. Report of an inquiry by Sir William Macpherson of Cluny*, consultabile al link *https://assets.publishing.service.gov.uk/media/5a7c2af540f0b645ba3c7202/4262.pdf,* 1999, 47,).

[8] MANNOZZI, *Razionalità e giustizia nella commisurazione della pena. Il Just Desert Model e la riforma del sentencing nordamericano,* cit., 377 ss.

[9] Sul punto, v. *amplius,* CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, cit., 81 ss.; CEVOLANI-CRUPI, *Come ragionano i giudici: razionalità, euristiche e illusioni cognitive*, in *disCrimen*, 2018, 8 ss.; *ivi* p. 22; BERTOLINO, *Problematiche neuroscientifiche tra fallacie cognitive e prove di imputabilità e di pericolosità sociale,* in *Dir. proc. pen.,* 2020, 1, 40 ss.; BLAIOTTA, *Giustizia, errore, intelligenza artificiale*, cit.; KANHEMAN-SLOVIC-TVERSKY, *Judgement under Uncertainty, Heuristics and Biases*, in *Cambridge University Press*, 1982.

[10] ANTIGONE, *Ventunesimo Rapporto sulle condizioni di detenzione.*

[11] Pur trattandosi di un numero abbastanza elevato, è interessante osservare come la percentuale di stranieri detenuti non superi mai il 10% della totalità delle presenze regolari sul territorio italiano e, anzi, a fronte della crescita esponenziale, negli ultimi anni, della popolazione straniera in Italia (da 3.891.295 nel 2009 a 5.141.341 nel 2024), la percentuale di quelli detenuti è scesa, essendosi il tasso di detenzione degli stranieri stabilito allo 0.37% nel 2023. Segno, tutto ciò, dell'inesattezza e pretestuosità delle campagne securitarie ed emergenziali legate alla presunta connessione tra maggiore presenza di immigrati sul territorio statale e conseguente crescita della criminalità. I detenuti stranieri, inoltre, rappresentano il 44,26% di coloro che sono condannati a meno di un anno di carcere, sintomo della minore accessibilità per gli stessi alle misure alternative alla detenzione rispetto agli italiani. (ANTIGONE, *Ventesimo Rapporto sulle condizioni di detenzione).*

[12] ANTIGONE, *Ventesimo Rapporto*, cit.

damentali degli individui è stata inizialmente concepita non solo con l'intento di velocizzare i relativi processi decisionali, ma proprio al fine di contenere la discrezionalità del decisore umano, tentando così di neutralizzare l'incidenza dei citati *bias* cognitivi e ridurre la componente discriminatoria delle decisioni mediante un processo di "*debiasing*", ossia attraverso l'individuazione di procedure e tecniche in grado di mitigare e contrastare l'influenza delle illusioni cognitive sulle determinazioni adottate[13]. Tale introduzione, tuttavia, pur facendo affidamento su strumenti e criteri apparentemente oggettivi, ha finito, spesso, per perpetuare e financo accentuare la citata disparità di trattamento tra bianchi e individui appartenenti a minoranze. Più in generale, l'utilizzo di metodi attuariali[14] nell'ambito della giustizia penale e della prevenzione di reati[15] ha, sin dal principio, suscitato non poche perplessità con riferimento, appunto, al conseguente aumento della componente discriminatoria delle decisioni assunte sulla base dei risultati ottenuti. Anche l'introduzione di sistemi tecnologici artificialmente intelligenti nasceva inizialmente per limitare la discrezionalità umana[16]. Lentamente, tuttavia, il coinvolgimento dell'IA nella formulazione di decisioni significative nella sfera dei diritti degli individui si è fatto sempre più preponderante, permeando, oltre che l'amministrazione della giustizia, altre funzioni pubbliche fondamentali come la sicurezza, la prevenzione dei reati, il controllo dei flussi migratori[17].

Si pone, dunque, un interrogativo di primaria rilevanza: in che misura un si-

---

[13] CEVOLANI-CRUPI, *Come ragionano i giudici: razionalità, euristiche e illusioni cognitive*, cit., 23.

[14] I metodi attuariali sono stati definiti come metodi che utilizzano «statistical methods – rather than clinical methods – on large datasets of criminal offending rates in order to determine the different levels of offending associated with a group or with one or more group traits and, on the basis of those correlations, to predict the past, present or future behavior of a particular person and to administer a criminal justice outcome for that individual» (cfr. HARCOURT, *Against Perdiction: Profiling, Policing, and Punishing in an Actuarial Age*, Chicago-London, 2007, 16).

[15] Tali metodi sono impiegati in Nordamerica per le più svariate funzioni: la previsione di possibili evasioni fiscali mediante il *Discriminant Index Function*, la profilazione dei corrieri della droga per efficientare i controlli negli aeroporti, la previsione di pericolosità per calcolare la durata delle misure cautelari custodiali, la lunghezza delle condanne a detenzione, la divisione nei circuiti carcerari e la concedibilità di misure alternative.

[16] Sul punto v. BACCARI-FELICIONI, *La decisione penale tra intelligenza emotiva ed intelligenza artificiale,* Padova, cit., 68; BLAIOTTA, *Giustizia, errore, intelligenza artificiale*, cit., 5; CARRATTA, *Decisione robotica e valori del processo penale*, cit., 94 s.

[17] ZUDDAS, *Intelligenza artificiale e discriminazioni*, in *Liber Amicorum per Pasquale Costanzo. Diritto Costituzionale in trasformazione. Vol. I – Costituzionalismo, Reti e Intelligenza Artificiale,* Genova, 2020, 457 ss.

stema standardizzato (tecnologico o meno che sia) può realmente garantire neutralità e imparzialità?[18]

Il presente contributo muove dal presupposto che l'integrazione di strumenti di IA nei processi decisionali delle autorità abbia spesso contribuito a cristallizzare e amplificare le pratiche discriminatorie di natura sistemica già radicate nella gestione, sia penale che amministrativa, dei soggetti appartenenti a minoranze etniche. È in tale prospettiva, dunque, che l'analisi intende focalizzarsi su un ambito che si configura, per la sua peculiare rilevanza empirica e giuridica, quale terreno privilegiato per l'indagine di fenomeni discriminatori: il trattamento riservato alle persone immigrate.

Benché un tale angolo prospettico possa – *prima facie* – apparire estraneo alle competenze del penalista, si impone tuttavia l'esigenza, sempre più avvertita, di superare una concezione riduttiva del diritto penale inteso unicamente come disciplina e studio della teoria del reato e della pena. Occorre, piuttosto, valorizzarne la dimensione assiologica, quale strumento volto alla tutela dei beni giuridici – e quindi dei diritti fondamentali della persona – in una prospettiva dinamica e anticipatoria, attenta all'individuazione dei profili di potenziale lesione (o pericolo di lesione) degli stessi, connessi ai mutamenti della società contemporanea, così da orientare l'elaborazione di strategie efficaci di prevenzione, in particolare sotto il profilo della prevenzione primaria. È noto come, infatti, le politiche securitarie succedutesi negli ultimi decenni abbiano lentamente marginalizzato la figura dello straniero[19], contribuendo

[18] Sul punto v. AIROLDI-GAMBETTA, *Sul mito della neutralità algoritmica*, in *Gli Algoritmi come costruzione sociale,* a cura di Martella-Campo-Ciccarese, in *The Lab's Quarterly*, 2018, a. XX, 4, 25 ss.

[19] Sul punto v. *amplius* LO MONTE, *Il fenomeno dell'immigrazione clandestina: diritti, sicurezza e criminalità*, in *La gestione dei flussi migratori tra esigenze di ordine pubblico, sicurezza interna ed integrazione europea. Atti del Convegno del Dipartimento di Diritto Pubblico e di Teoria e Storia delle Istituzioni,* a cura di Stasi-Kalb, Salerno, 24 maggio 2012, 135 ss.; DAL LAGO, *Non-persone. L'esclusione dei migranti in una società globale,* Milano, 1999, 63 ss.; DONINI, *Il cittadino extracomunitario da oggetto materiale a tipo d'autore nel controllo penale dell'immigrazione,* in *Questione Giustizia,* 1, 101 ss; MASERA, *La crimmigration nel Decreto Salvini,* in *Leg. pen.,* 24 luglio 2019; GATTA, *La pena nell'era della 'crimmigration': tra Europa e Stati Uniti*, in *La pena, ancora: tra attualità e tradizione. Scritti in onore di Emilio Dolcini,* a cura di Paliero-Viganò-Basile-Gatta, Milano, 2018, 987 ss.; SPENA, *La crimmigration e l'espulsione dello straniero-massa*, in *Materiali per una storia della cultura giuridica*, 2017, 2, 495 ss.; DI MARTINO-BIONDI DAL MONTE-BOIANO-RAFFAELLI, *The criminalization of irregular immigration: law and practice in Italy*, Pisa, 2013.

all'insorgere del fenomeno della "*crimmigration*"[20], il quale presenta rilevanti implicazioni dal punto di vista penalistico. Risulta, pertanto, di particolare interesse indagare le intersezioni tra l'assetto repressivo proprio della *crimmigration* e la progressiva "algoritmizzazione" delle pratiche di governo, controllo e gestione dei flussi migratori.

A tal fine, si procederà in primo luogo (paragrafi 2 e 3) ad analizzare, in generale, le ragioni per cui i sistemi di IA causano discriminazione, concentrandosi in particolare su due tipologie di *software*: a) algoritmi predittivi che, a seguito dell'immissione da parte del soggetto umano di una molteplicità di dati personali riferibili ad un individuo, passando per una «sequenza di passaggi elementari»[21], formulano una previsione avente ad oggetto un certo *output* richiesto dall'umano manovrante, come ad esempio la probabilità di futura commissione di reati o di violazione di prescrizioni comportamentali da parte di quell'individuo[22], che verrà poi utilizzato dal soggetto competente per indirizzare il proprio operato; b) sistemi di sorveglianza basati su tecnologie di riconoscimento facciale e categorizzazione biometrica[23], che permettono una sorveglianza mirata nei confronti della popolazione, ed in particolare di quelle fasce di essa considerate più pericolose.

Una volta delineati tali effetti, si affronteranno in particolare le problematiche per i diritti fondamentali dei migranti conseguenti all'impiego di detti strumenti nel settore specifico del controllo delle frontiere e alla connessione di tale ambito con quello della tutela della pubblica sicurezza e della prevenzione dei reati (paragrafo 4). Infine, si procederà all'analisi del Regolamento n.

---

[20] Termine reso popolare da Juliet Stumpf, Professoressa di diritto presso la Lewis e Clark Law School, nel suo articolo *The Crimmigration Crisis: Immigrants, Crime and Sovereign Power,* in *American University Law Review,* 2006, vol. 52, 2, 367 ss.

[21] NATALE, *Intelligenza artificiale, neuroscienze, algoritmi. Aggiornato al nuovo regolamento Ai Act,* Pisa, 2024, 1.

[22] Si fa riferimento all'ambito di interesse, ma in altre materie possono trovarsi sistemi che formulano le previsioni più disparate. Alcuni algoritmi sono stati creati, ad esempio, per prevedere la data di morte del soggetto immettente i dati, sulla base delle sue abitudini di vita e dei suoi dati sanitari (cfr. https://life2vecai.com/)

[23] Per categorizzazione biometrica si intende l'assegnazione, mediante un sistema tecnologico, di persone fisiche a categorie specifiche sulla base dei loro dati biometrici. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti comportamentali o di personalità, la lingua, la religione, l'appartenenza a una minoranza nazionale, l'orientamento sessuale o politico.

2024/1689 del 13 giugno 2024 (d'ora in poi AI Act) e della recentissima legge che ne recepisce i contenuti nel nostro ordinamento: la L. 23 settembre 2025 n. 132, con l'obiettivo di valutare se l'impianto normativo risultante dalla loro combinazione offra strumenti efficaci nel contrastare le citate distorsioni, permettendo un impiego equo e non pregiudiziale dell'intelligenza artificiale nel campo interessato (paragrafi 5 e 6).

2. *Algoritmi predittivi.* Prima di affrontare l'annunciata analisi critica, occorre brevemente comprendere il funzionamento delle tecnologie di cui si vuole trattare, nonché le ragioni sottostanti alla compressione dei diritti fondamentali che, in termini generali, può derivare dall'utilizzo delle stesse.
Come noto, la sostanza dell'intelligenza artificiale, il suo «tessuto costitutivo»[24], è formato da neuroni artificiali, che compongono reti neurali artificiali ispirate a quelle biologiche[25], le quali imparano a svolgere dei compiti rifacendosi ad esempi. Esse si organizzano su un dato numero di strati (*layers*): l'*input layer*, composto da neuroni che ricevono dati (*input*) dall'esterno, che vengono processati, trasformati in informazioni, e trasferiti ai neuroni che formano *l'hidden layer*, che elabora le informazioni ricevute e le invia ad altri *hidden layers*, che le elaborano ancora, fino ad arrivare all'ultimo stato, l'*output layer,* che fornisce la risposta definitiva[26]. Più *hidden layers* vi sono, più il sistema è intelligente ed in grado di fornire risposte accurate ed attendibili. È quindi imprescindibile che il sistema riceva, per poter svolgere i suoi compiti, delle istruzioni di base e dei dati di addestramento (per questo di parla di "*machine learning*"[27]).

[24] ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. proc.,* 2021, 6, 726; BACCARI-FELICIONI, *La decisione penale tra intelligenza emotiva ed intelligenza artificiale,* cit., 72.
[25] COMMISSIONE EUROPEA PER L'EFFICIENZA DELLA GIUSTIZIA, *Carta etica per l'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, 3 dicembre 2018, 48 (voce: NEURONI/RETI NEURALI).
[26] BACCARI-FELICIONI, *La decisione penale tra intelligenza emotiva ed intelligenza artificiale,* cit., 74.
[27] «L'apprendimento automatico consente di costruire, a partire dai dati, un modello matematico che include un gran numero di variabili non conosciute in anticipo. I parametri si configurano gradualmente durante la fase di apprendimento, che utilizza insiemi di dati di addestramento per reperire e classificare i collegamenti. I diversi metodi di apprendimento automatico sono scelti dai progettisti a seconda della natura dei compiti da svolgere (raggruppamento). Tali metodi sono generalmente classificati in tre categorie: apprendimento supervisionato (da un essere umano), apprendimento non supervisionato e apprendimento per rinforzo. Queste tre categorie raggruppano differenti metodi tra cui le reti neurali,

Per quanto qui di interesse, quando facciamo riferimento agli algoritmi predittivi, l'*output* corrisponde ad una previsione sul futuro comportamento di un dato soggetto, formulata sulla base di suoi dati personali e delle "conoscenze" maturate dall'algoritmo grazie ai dati di addestramento. Tali algoritmi, più propriamente denominati *risk-assessment tools*, sono attualmente impiegati in diversi ordinamenti da parte degli operatori istituzionali (autorità di pubblica sicurezza, forze di polizia, giudici, ecc.), per effettuare previsioni statistiche a supporto delle proprie decisioni.

Un primo esempio in tal senso si rinviene nell'impiego dell'intelligenza artificiale nel campo della prevenzione penale[28], attraverso la cosiddetta "polizia predittiva"[29], definibile come «Qualsiasi strategia o tattica di polizia che sviluppi e utilizzi informazioni e analisi avanzate per guidare una prevenzione del crimine proattiva»[30]. Questa può avere due obiettivi diversi, distinguendosi sul punto tra i sistemi *place-based*, che elaborano previsioni individuando le aree cittadine in cui potrebbero essere commessi reati, e quelli *person-based*, che forniscono una valutazione del rischio individuale, identificando i soggetti più propensi a commettere illeciti in futuro[31]. Altro esempio è l'impiego degli al-

---

l'apprendimento profondo, ecc.» (CEPEJ, *Carta etica per l'uso dell'intelligenza artificiale*, cit., 45).

[28] SIGNORATO, *Giustizia Penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. proc.*, 2020, 607.

[29] Sulla *predictive policing* in generale v. FERGUSON, *The Rise of Big Data Policing: Surveillance, Race and the Future of Law Enforcement,* New York, 2017; JOH, *Ethical AI in American Policing,* in *Notre Dame Journal on Emerging Technologies,* 2022, vol. 3, 2, 262 ss.; SIGNORATO, *Giustizia Penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, cit.; PIETROCARLO, *Predictive policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali,* in *www.sistemapenale.it*, 28 settembre 2023.

[30] ELECTRONIC PRIVACY INFORMATION CENTER, *Algo-rhytms in the Criminal Justice System*, (https://epic.org/issues/ai/ai-in-the-criminal-justice-system/).

[31] Fu il dipartimento di polizia di Santa Cruz in California uno dei primi a testare un programma di polizia predittiva, chiamato PredPol e sviluppato da un'azienda privata (cfr. GOOD, *Sending the Police Before There's a Crime*, in *The New York Times*, 15 agosto 2011). Più recente è la Strategic *Suspect List* di Chicago, che raccoglie dati relativi a persone già coinvolte, in qualche modo, in vicende giudiziarie, siano esse autori o vittime di reati e a partire da questi soggetti, l'indagine si estende progressivamente a tutte le persone in contatto con esse, o comunque orbitanti nella loro sfera relazionale, per fornire infine una lista di soggetti ("*heat list*") potenzialmente a rischio di commissione di fatti illeciti nel prossimo futuro, che viene quindi attenzionata dalla polizia (cfr. PIETROCARLO, *Predictive policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali,* cit.). Per un panorama generale su tutte le agenzie che al 2022 utilizzavano sistemi di tal genere negli Stati Uniti v. ELECTRONIC FRONTIER FOUNDATION, *Atlas of Surveillance*, consultbile al link https://atlasofsurveillance.org/atlas). In Italia il primo esperimento fu messo in atto da varie Questure attraverso l'impiego dei *software* Keycrime e XLAW, entrambi volti, in modo differente, a calcolare le aree cittadine a rischio di commissione di rea-

goritmi nell'ambito della decisione giudiziale per calcolare la probabilità di recidiva di soggetti sottoposti a procedimento. Emblematica in tal senso è la sentenza della Corte suprema degli Stati Uniti nel caso Wisconsin S.C. State v. Loomis (conosciuto anche come Caso COMPAS), giunto dinanzi la Corte suprema americana. Evitando di ripercorrerne analiticamente i passaggi salienti, già ampiamente approfonditi dalla dottrina specialistica[32], basti ricordare che in tale procedimento, nel computo della pena, i giudici avevano tenuto conto dei risultati elaborati dal *software* di IA COMPAS (*Correctional offender management profiling for alternative sanctions*[33]), secondo cui l'imputato doveva considerarsi un soggetto ad alto rischio di recidiva sulla base dell'analisi di diversi parametri, ritenuti dalla difesa di Loomis discriminatori e poco trasparenti (età, lavoro, vita sociale e relazionale, grado di istruzione, etnia, ecc[34].).

Orbene, può dirsi che gli effetti indesiderati e discriminatori degli algoritmi derivino da vari e numerosi fattori e possano avere origine in diverse fasi del processo di progettazione e funzionamento del sistema intelligente[35].

Per quanto riguarda il momento in cui le distorsioni discriminanti possono verificarsi, innanzitutto esse possono avere origine durante la fase di costruzione dell'algoritmo[36], a causa di credenze personali e pregiudizi del progetta-

---

ti (sul punto v. LOMBARDO, *Sicurezza 4P. Lo studio alla base del software XLAW per prevedere e prevenire i crimini,* Venezia, 2019; SIGNORELLI, *Il software italiano che ha cambiato il mondo della polizia predittiva,* in *www.wired.it*, 2019; ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. proc.,* 2021, 6, 724 ss.). In Germania, dal 2017 il Buneskriminalamt utilizza lo strumento RADA-iTE per differenziare i militanti Salafisti in livelli di pericolosità, mentre la Bavaria utilizza lo strumento PRECOBS per calcolare i luoghi dove vi è probabilità che vengano commessi furti in appartamento (cfr. ALGORITHM WATCH, *Automating Society Report 2020 – Germany Section*, consultabile al link https://automatingsociety.algorithmwatch.org/report2020/germany/).

[32] BACCARI-FELICIONI, *La decisione penale tra intelligenza emotiva ed intelligenza artificiale,* cit., 78; CARRER, *Se l'amicus curiae è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin*, in *www.giurisprudenzapenale.com*, 2019, 4; *Criminal Law – Sentencing Guidelines, Wisconsin Supreme Court Requires Warnings before Use of Algorithmic Risk Assessment in Sentencing. – State v. Loomis,* 881 N. W. 2d 749 (Wis. 2016), in *Harward Law Review,* 130, n. 5, 2017, 1530 ss.

[33] Prodotto e brevettato dalla compagnia privata Northpointe, che vanta il segreto industriale su tutte le componenti del sistema.

[34] Assieme ai dati personali il *software* valuta anche le risposte ad un questionario di più di cento domande, tra le quali alcune formulate come segue: 1) Quanti dei tuoi amici sono stati arrestati? 2) Sei mai stato sospeso o espulso da scuola? 3) Quanto spesso ti senti annoiato?.

[35] ZUDDAS, *Intelligenza artificiale e discriminazioni*, cit., 461.

[36] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*,

tore[37]. Successivamente, i *bias* possono emergere nella fase di selezione delle categorie di dati che l'algoritmo dovrà elaborare o nei dati utilizzati per l'allenamento[38]. Sotto tale ultimo aspetto, l'accuratezza degli algoritmi può essere compromessa ove i dati di allenamento non siano sufficientemente rappresentativi[39]. Maggiore sarà il pluralismo dei dati utilizzati nella fase di *training*, maggiore sarà l'accuratezza del sistema[40]. Da ultimo, le discriminazioni possono derivare anche da decisioni "autonome" dell'algoritmo che, individuando determinate caratteristiche in alcuni individui, associno loro un trattamento deteriore[41].

Deve osservarsi, dunque, come a giocare un ruolo preponderante siano principalmente la tipologia e la qualità dei dati che vengono coinvolti nel funzionamento dell'algoritmo, sia in fase di addestramento che di funzionamento. I *risk assesment tools*, infatti, raramente comportano una discriminazione c.d. diretta, ossia un trattamento differenziato esplicitamente giustificato sulla base di caratteristiche proprie di una determinata categoria di persone. Piuttosto, essi tendono a configurare forme di discriminazione di tipo indiretto o "per *proxy*", consistenti in decisioni solo formalmente neutrali, ma in realtà influenzate da variabili che fungono da indicatori surrogati di caratteristiche riconducibili a categorie protette, ovvero che riflettono attributi distintivi giuridicamente non rilevanti o, comunque, non legittimamente utilizzabili a fini decisionali[42].

Oltre a tipologia e qualità, fondamentale risulta anche la modalità in cui dati di addestramento vengono raccolti. Essi provengono, infatti, da una vastissima gamma di fonti, che spaziano dal *web*, alle *app* utilizzate sui dispositivi mobili. Molti dati derivano anche da altri algoritmi (negli Stati Uniti, sul punto, si è

Napoli, 2021, 219.

[37] ZUDDAS, *Intelligenza artificiale e discriminazioni*, cit., 461.

[38] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 221.

[39] Se i dati sono discriminatori perché non sufficientemente rappresentativi si parla di "*bias* di selezione", mentre se la distorsione deriva dal riflettersi di un pregiudizio appartenente al soggetto responsabile dell'immissione dei dati, si parla di "*bias* di conferma".

[40] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 221.

[41] ZUDDAS, *Intelligenza artificiale e discriminazioni*, cit., 461.

[42] ZUDDAS, *Intelligenza artificiale e discriminazioni*, cit., 462.

parlato di «algoritmi criminalizzanti»[43]) impiegati in settori come l'edilizia abitativa, l'assistenza sanitaria, l'istruzione, la concessione di credito, l'immigrazione ed altri[44]. Essi elaborano informazioni relative principalmente alle condizioni socio-economiche degli individui, al loro luogo di residenza, etnia, *background* familiare, occupazione e reti sociali, influenzando le informazioni detenute dalle autorità, codificano il razzismo sistemico e contribuendo, oltre che alla creazione di disuguaglianze nel contesto dello sviluppo sociale e nell'accesso ai servizi pubblici[45], anche all'avvicinamento e all'ingresso di soggetti emarginati nel sistema della giustizia penale[46].

I dati utilizzati dagli algoritmi predittivi provengono anche da strumenti di sorveglianza progettati per osservare, tracciare e archiviare informazioni sulle persone. In Nordamerica, ad esempio, un'inchiesta del Wall Street Journal su Premise – un'applicazione per dispositivi mobili che paga i privati per raccogliere informazioni e scattare foto delle loro zone residenziali – ha svelato come le autorità di polizia utilizzino le immagini raccolte dall'azienda per addestrare algoritmi predittivi[47]. Inoltre, è diventata comune la pratica, da parte delle forze di polizia, di impiegare immagini registrate dai campanelli "*smart*" delle abitazioni private[48].

---

[43] ELECTRONIC PRIVACY INFORMATION CENTER, *Algo-rhytm,* cit.

[44] Prassi vigente in molti altri paesi, come la Danimarca, dove è stata di recente adottata una normativa di potenziamento delle capacità di intrusione della forza pubblica nei dati personali mediante la piattaforma POL-INTEL, che agisce mediante l'incrocio di dati provenienti da videocamere, *social networks*, internet ed altro, con quelli presenti nelle banche dati della polizia, oppure la Cina, ove mediante il sistema Police Cloud System le forze dell'ordine mettono in atto una sorveglianza continua sulla popolazione attraverso l'incrocio tra dati abitualmente raccolti dalla polizia e dati provenienti da altri dipartimenti del Governo e perfino da compagnie private (cfr. BONFANTI, *Big Data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *www.medialaws.eu,* 2018, 3, 207 ss).

[45] Proprio il Parlamento europeo ha affermato: «big data may result not only in infringements of the fundamental rights of individuals, but also in differential treatment of and indirect discrimination against groups of people with similar characteristics, particularly with regard to fairness and equality of opportunities for access to education and employment, when recruiting or assessing individuals or when determining the new consumer habits of social media users» (EUROPEAN PARLIAMENT, *Report on Fundamental Righst Implication of Big Data: privacy, data protection, non-discriminations, security and law enforcement,* 20 febbraio 2017).

[46] ELECTRONIC PRIVACY INFORMATION CENTER, *Algo-rhytms,* cit.

[47] TAU, *App Taps Unwitting Users Abroad to Gather Open-Source Intelligence*, in *The Wall Street Journal,* 24 giugno 2021.

[48] Citofoni di marca Ring (Amazon) o Nest (Google) che prevedono anche apposite applicazioni, come *Neighbors*, le quali consentono agli abitanti di un dato quartiere di stilare una lista di persone sospette

I dati così raccolti consentono la profilazione della popolazione[49]: una volta collezionati vengono raggruppati in profili basati su specifici aspetti della persona; le persone che condividono più caratteristiche vengono associate a un determinato profilo ed infine, attraverso calcoli probabilistici, l'algoritmo inferisce la sussistenza di tratti comuni e ricorrenti tra gli individui appartenenti a uno stesso profilo[50], pur in assenza di un riscontro diretto[51].

La crescente importanza e capacità predittiva dei *risk assesment tools* è quindi strettamente legata all'avvento dei *big data*[52] e a quello che è stato definitivo come «data fundamentalism»[53], fenomeno che vede la società permeata da informazioni e previsioni basate su una quantità di dati inimmaginabile[54] che,

---

avvistate tramite il dispositivo telematico. In base a quanto riportato in un'inchiesta di Vice del 2019, la grande maggioranza delle persone inserite di tali liste erano persone di colore (cfr. VICE, *How Ring Transmits Fear to American Suburbs*, 6 dicembre 2019, consultabile al link *https://www.vice.com/en/article/how-ring-transmits-fear-to-american-suburbs/).*

[49] Sul punto v. *amplius* LAGIOIA-SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *www.federalismi.it*, 2020, 11, 85 ss., FERRARIS, *La profilazione e i suoi rischi,* in *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, a cura di Brighi-Zullo, Roma, 2015, 70.

[50] «Un sistema di profilazione stabilisce (prevede) che gli individui con determinate caratteristiche C1, hanno anche una certa probabilità di possedere alcune caratteristiche aggiuntive C2. Si consideri, per esempio, il caso di un sistema che stabilisca (predica) che coloro che presentano certe caratteristiche genetiche hanno anche la tendenza a sviluppare il cancro con una probabilità superiore alla media, o che gli individui con una certa istruzione e un certo storico lavorativo o che appartengono a una certa etnia, hanno anche una probabilità superiore alla media di inadempienza dei propri debiti. In questi casi, è possibile affermare che il sistema in esame ha profilato il gruppo di individui che possiedono le caratteristiche C1, aggiungendo un nuovo segmento di informazioni alla descrizione (il profilo) di tale gruppo, vale a dire la probabilità di possedere le caratteristiche aggiuntive C2. Successivamente, indicando al sistema che un soggetto possiede le caratteristiche C1, il sistema sarà in grado di inferire che, con una certa probabilità, quel determinato soggetto possiederà anche le caratteristiche aggiuntive C2.» (LAGIOIA-SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, cit., 90).

[51] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 202.

[52] Nella definizione fornita dal Parlamento europeo nel già citato *Report on Fundamental Righst Implication of Big Data:* «big data refers to the collection, analysis and the recurring accumulation of large amounts of data, including personal data, from a variety of sources, which are subject to automatic processing by computer algorithms and advances data-processing techniques using both stored and streamed data in order to generate certain correlations, trends and patterns (big data analytichs)».

[53] CRAWFORD, *The Hidden Biases in Big Data*, in *Harvard Business Review*, 1 aprile 2023.

[54] Oltre a distinguersi dagli altri aggregati di dati per volume e varietà delle fonti, i *big data* mostrano il lato più innovativo sul piano qualitativo, permettendo – tramite la loro consultazione – la desunzione di informazioni sempre più precise e finalizzate ad una pluralità indeterminata di scopi. (così G. DELLA MORTE, *La regolazione dell'AI: profili internazionalistici*, in *La disciplina dell'intelligenza artificiale,* a cura di Finocchiaro-Palmirani-Pollicino-Vaciago-Ziccardi, Milano, 2025, 70).

tuttavia, nasconde innumerevoli problematiche giuridiche[55].

Certamente, i *big data* sono intimamente connessi alla cultura, ai luoghi fisici abitati dalle persone, alle loro abitudini e alla loro classe sociale, ed inevitabilmente ne riflettono le disuguaglianze[56]. Seppure, quindi, in nessun caso i dati immessi in un certo algoritmo siano intenzionalmente discriminatori, sarà proprio la capacità analitica del sistema di intelligenza artificiale a portare alla luce e "restituire" discriminazioni latenti, radicate nel tessuto sociale di riferimento[57], nonché i sistemi di valori e le intenzioni del creatore stesso del sistema[58]. È ormai pacifico che, al di là della retorica della neutralità algoritmica, i sistemi di intelligenza artificiale costituiscano veri e propri prodotti storici e sociali che, in quanto tali, incorporano e riflettono gli assunti culturali, i *bias,* e le dinamiche di potere proprie delle strutture sociali in cui vengono progettati e impiegati[59].

Se, ad esempio, un algoritmo destinato a prevedere in quali zone della città si commetteranno più reati venisse addestrato con le informazioni contenute in un *database* della polizia in cui la percentuale di immigrati è superiore a quella del resto della popolazione, il sistema di *machine learning* apprenderebbe

---

[55] Sulle problematiche di compatibilità con la normativa sulla *data protection* v. la Direttiva (UE) n. 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati ed il già citato Report on Fundamental Righst Implication of Big Data del Parlamento europeo. Per un'analisi approfondita del problema v. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018; *La protezione dei dati personali ed informativi nell'era della sorveglianza globale*, a cura di Distefano, Napoli, 2017; BONFANTI, *Big Data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali,* cit.; BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati,* in *Cybercrime*, a cura di Cadoppi-Canestrari-Manna-Papa, Vicenza, 2023, 1868 ss.; DE TULLIO, *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Pol. Dir.,* 2016, 4, 637 ss.

[56] K. Craword fa l'esempio dell'*app* StreetBump, utilizzata dall'amministrazione della città di Boston per calcolare, attraverso i dati del Gps, la presenza di buche sul manto stradale che, sebbene ingegnosa, si è dimostrata inefficace in quanto una parte significativa della popolazione cittadina, soprattutto quella abitante in zone della città più disastrate, non possedeva uno smartphone perché indigente o, semplicemente, anziana, risultando di fatto esclusa dalla possibilità di utilizzo dell'applicazione (CRAWFORD, *The Hidden Biases in Big Data*, cit.).

[57] PELUSO, *Intelligenza artificiale e dati di qualità: la tecnologia come valido alleato*, in *www.medialaws.eu,* 2022, 2.

[58] SIGNORATO, *Giustizia Penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, cit., 614.

[59] AIROLDI-GAMBETTA, *Sul mito della neutralità algoritmica*, cit., 27.

che gli immigrati sono più propensi a commettere crimini[60]. Di conseguenza, la forte concentrazione etnica in alcune aree urbane, unita a condizioni di disagio economico, porterebbe l'algoritmo a considerare queste zone ad alto rischio. Tale previsione si tradurrebbe in un maggiore controllo da parte della polizia, con un conseguente aumento del tasso di arresti, il che, a sua volta, incrementerebbe il punteggio criminale della zona, generando un circolo vizioso che si concluderebbe con la ghettizzazione e discriminazione di intere aree cittadine, a causa, principalmente, della loro composizione etnica e dei pregiudizi legati alla provenienza geografica degli abitanti[61], in un fenomeno noto come «*self-fulfilling prophecy*»[62]. La qualità del risultato fornito dall'algoritmo non può che dipendere, in definitiva, dalla qualità dei dati immessi nell'*input layer*[63].

Va aggiunta, poi, ai fattori determinanti le conseguenze pregiudizievoli descritte, l'eccessiva automaticità della decisione algoritmica che, seppur logicamente "esatta" poiché aderente ai dati forniti e consistente nell'unica soluzione inferenziale possibile, può condurre a risultati formalmente razionali ma so-

[60] ZUDDAS, *Intelligenza artificiale e discriminazioni*, cit., 466.

[61] PIETROCARLO, *Predictive policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali,* cit.

[62] BACCARI-FELICIONI, *La decisione penale tra intelligenza emotiva ed intelligenza artificiale,* cit. 95.
Sul punto, interessante la riflessione di Harcourt sugli effetti sociali e criminologici dell'utilizzo di metodi predittivi in campo penale ove osserva che «Disproportionate criminal supervision and incarceration reduces work opportunities, breaks down families and communities, and disrupts education. It contributes to the exaggerated general perception of the criminality of the targeted group in the public imagination and among law enforcement officers. This, in turn, further undermines the ability of the targeted group to obtain employment or pursue educational opportunities. It may also have a delegitimizing effect on the criminal justice system that may lead disaffected members of the profiled group to greater disregard of the criminal law in a kind of blacklash against perceived or real prejudice. And it may corrode community-police relations, hampering law enforcement efforts as members of the profiled community become less willing to report crime, to testify, and to convict. In this sense, the use of actuarial methods in the criminal justice context can affect a person's life-course in extremely detrimental ways. It can result in self-fulfilling effects on employment, education, and family» (HARCOURT, *Against Perdiction,* cit., 29). Meritano menzione, poi, le teorie sociologiche del controllo sociale e della privazione relativa sulla connessione tra immigrazione e criminalità, secondo cui sarebbe proprio il contesto sociale ostile ed i continui controlli messi in atto nei loro confronti dalle forze di polizia ad indurre gli immigrati a trasgredire le norme, non riponendo fiducia nello Stato, percepito come ingiusto e indegno di lealtà (cfr. BECCUCCI, *Immigrazione e criminalità in Italia. Un esempio di "cortocircuito" teorico interpretativo della ricerca sociale,* in *Immigrazione illegale e diritto penale. Un approccio interdisciplinare*, a cura di Rosi-Rocchi, Napoli, 2013, 306).

[63] Nel campo dell'informatica, questo fenomeno è noto come "GIGO" (*garbage in, garbage out*): dati difettosi in ingresso producono risultati senza senso in uscita.

stanzialmente privi di senso[64], forieri di errori che, all'occhio umano, risultano grossolani[65]. Poiché, infatti, si tratta di decisioni basate su grandi quantità di dati – che tendono a restituire la risposta più probabile – esse non derivano da una comprensione del percorso seguito per giungere al risultato, ma semplicemente da un'interazione inconsapevole tra dati[66]. La mancanza, da parte dell'algoritmo, di senso comune, di coscienza, di cooperazione tra sfera emozionale e razionale[67], di «autonomia cognitiva»[68], lo priva della piena comprensione del senso delle situazioni, rendendo a sua volta inconoscibile il procedimento logico seguito per giungere alla soluzione[69]. Ne consegue l'enorme difficoltà nel risalire a quale delle possibili variabili, in una fittissima rete di connessioni, abbia avuto un peso maggiore e determinante nella decisione finale della macchina[70]. L'estrema opacità del percorso seguito dall'algoritmo per giungere al risultato finale ha portato al celebre paragone del suo funzionamento con una *black box*[71], inaccessibile all'occhio e all'intelletto umano.

In materia di diritti fondamentali, quindi, non può non notarsi come siano le intrinseche caratteristiche delle stesse decisioni giuridiche che mal si conformano ad essere oggetto di elaborazioni algoritmiche, poggiando il diritto su interpretazioni frutto di ragionamenti ancorati a principi, come l'equità, l'uguaglianza, la proporzionalità, che sfuggono alla comprensione del *soft-*

---

[64] BLAIOTTA, *Giustizia, errore, intelligenza artificiale*, cit., 11.

[65] Sul punto, e più in generale sulla problematica della c.d. "scorciatoia" – definita dall'Autrice come la «tendenza degli algoritmi di machine learning a trovare soluzioni semplificate per risolvere un compito, sfruttando correlazioni spurie» – v. FRAGASSO, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile",* cit., 33 ss.

[66] BACCARI-FELICIONI, *La decisione penale tra intelligenza emotiva ed intelligenza artificiale,* cit., 83.

[67] BLAIOTTA, *Giustizia, errore, intelligenza artificiale*, cit.,11.

[68] MANTOVANI, *L'utilizzo dell'I.A. nella formazione della decisione penale*, in *Intelligenza Artificiale, Diritto, giustizia, economia ed etica,* a cura di Basile-Biasi-Camaldo-Caneschi, Fragasso-Milani, cit., 96. Ricorda l'Autrice che «La simulazione di un processo cognitivo non produce, dunque, i medesimi risultati che conseguono a una reazione neurofisiologica, come accade nella mente di un soggetto pensante. Conseguentemente, pur avvalendosi di canoni di certezza logico probabilistica e di un ragionamento di tipo inferenziale, gli algoritmi predittivi non sarebbero in grado in ricostruire tutte le sfumature proprie della scienza giuridica, pervenendo esclusivamente a una valutazione della ripetitività di una condotta giuridicamente rilevante, nota ma non necessariamente reiterabile in futuro» (*Id.*, 97).

[69] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 41.

[70] PELUSO, *Intelligenza artificiale e dati di qualità: la tecnologia come valido alleato*, cit.

[71] DONATI, *Intelligenza artificiale e diritti fondamentali nel regolamento sull'intelligenza artificiale*, in *La disciplina dell'intelligenza artificiale,* a cura di Finocchiaro-Palmirani-Pollicino-Vaciago-Ziccardi, cit., 43.

ware[72].

3. *Non solo algoritmi predittivi: i sistemi di sorveglianza intelligenti e il riconoscimento facciale.* Passando al secondo gruppo oggetto di analisi, i sistemi di riconoscimento facciale possono essere definiti come *software* che, attraverso complessi procedimenti algoritmici che elaborano immagini[73], permettono di confrontare l'identità di un volto ignoto con quella di milioni di soggetti presenti in un *database* in uso all'operatore[74]. Tali sistemi fanno parte del più ampio gruppo delle tecnologie biometriche, che includono tutti i sistemi che consentono di distinguere, per specifiche finalità, un soggetto dagli altri attraverso l'analisi di caratteristiche fisiche uniche, come l'iride, le impronte digitali o, addirittura, tratti comportamentali come il modo di camminare[75]. Detti sistemi "vedono" le immagini tramite un approccio "*bottom-up*" basato sul *machine-learning*. In altre parole, sono in grado di imparare autonomamente, a partire da un *dataset* di immagini fornitegli, a riconoscere un volto e le sue caratteristiche somatiche[76].

Detti sistemi possono essere utilizzati per diverse finalità, tra cui: confermare l'identità di un soggetto (*facial identification* o *verification*); svolgere compiti di sorveglianza generale, identificando molte persone contemporaneamente in luoghi pubblici come aeroporti o strade[77] (*facial surveillance*[78]); classificare

---

[72] Così SIGNORATO, *Giustizia Penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo,* cit., 611.

[73] È stata proposta una divisione in sequenza per spiegare l'algoritmo di riconoscimento facciale, predisposta come segue: a) fase di acquisizione dell'immagine, consistente nella conversione in formato digitale del volto di una persona acquisita con o senza il consenso di quest'ultima; b) fase di individuazione di un volto, consistente nel momento in cui l'immagine del volto viene isolata dallo sfondo; c) fase di normalizzazione, consistente nell'attenuazione delle variazioni presenti all'interno del volto; d) fase di estrazione delle caratteristiche, finalizzata ad isolare le caratteristiche biometriche distintive della persona rappresentata che creeranno il cosiddetto *template* biometrico, ovvero un'immagine vettoriale di riferimento che verrà successivamente impiegata per il confronto con altri *template*; e) fase di registrazione dell'immagine o del modello nel *database*; f) fase di confronto, consistente nella misurazione delle somiglianze tra i tratti biometrici del modello di riferimento con quelli di altri modelli già registrati. (Cfr. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 32 ss.).

[74] BACCARI-FELICIONI, *La decisione penale tra intelligenza emotiva ed intelligenza artificiale,* cit., 96.

[75] Così MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 11.

[76] *Ibid.,* 52.

[77] JOH, *Ethical AI in American Policing,* cit., 269.

soggetti in base a caratteristiche come il sesso, l'età, l'etnia (categorizzazione biometrica). Una finalità sviluppatasi più di recente, soprattutto in ambito commerciale ma poi estesasi anche in campo penale e specialmente in fase di interrogatorio, è l'analisi delle emozioni[79].

Attraverso le tecnologie biometriche possono raggiungersi gli stessi obiettivi di profilazione di cui si parlava *supra*: l'algoritmo di riconoscimento, infatti, isola una o più caratteristiche di un soggetto per ricondurlo ad un determinato profilo[80]. Analogamente a quanto accaduto con i *risk assesment tools*, le autorità dei paesi più sviluppati hanno iniziato ad utilizzare le tecnologie biometriche in ambito pubblico[81] sin dagli anni '90, impiegandole in una vasta gamma di settori, tra cui l'attività preventiva e investigativa delle forze dell'ordine[82], la ricerca di persone scomparse, la raccolta di prove nei procedimenti penali[83], la gestione delle politiche migratorie e di rimpatrio, nonché i controlli alle fron-

---

[78] Differenziazione delineata da GARVIE-BEYODA-FRANKLE, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, in *www.perpetuallineup.org,* 2016.

[79] Per un approfondimento sul punto si rimanda a LI-HONG-MOILANEN-HUANG-PFISTER-ZHAO, *Towards Reading Hidden Emotions: A Comparative Study of Spontaneous Micro-Expression Spotting and Recognition Methods*, in ÆEE Transactions on Affective Computing**,** 2018, vol. 9, 4, 563-577; GIFFORD, *The Problem with Emotion-Detection Technology,* in *TheNewEconomy.com*, 15 giugno 2020.

[80] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 203.

[81] Per una panoramica sul diffusissimo utilizzo, invece, in ambito privato e commerciale v. U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Use*, GAO-20-522, 2020.

[82] Esempio più celebre è sicuramente l'impiego da parte della South Wales Police del sistema di riconoscimento facciale denominato AFR Locate nell'attività di prevenzione dei reati, che ha portato alla sentenza della *High Court of Justice* del Regno Unito del 2019, ampiamente commentata anche dalla dottrina italiana (cfr. DELLA TORRE, *Novità del Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Dir. pen. cont.,* 2020, 1, 231 ss). Per una panoramica sui paesi e le autorità di *law enforcement* che utilizzano sistemi di riconoscimento facciale, v. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *Facial Recognition technology: fundamental rights considerations in the context of law enforcement*, 27 novembre 2019, 11 ss.; KAISER-BRIL, *At least 11 police forces use face recognition in the Eu, AlgorithmWatch reveals*, in *www.algorithmwatch.org,* 18 giugno 2020.

[83] A riguardo v., *amplius*, HUANG-XIONG-ZHANG, *Face Recognition Applications*, in *Handbook of Face Recognition,* a cura di Li-Jain, Seconda Edizione, Pechino, 2011, 617 ss; LOPEZ, *La rappresentazione facciale tramite software*, in *Le indagini atipiche*, a cura di Scalfati, Torino, 2019, 239 ss.; SACCHETTO, *Face to Face: il complesso rapporto tra automated faciale recognition technology e processo penale,* in *Leg. pen.*, 2020; DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale*?, in *Intelligenza artificiale e processo penale. Indagini, prove, giudizio,* a cura di Pressacco-Di Paolo, cit., 7 ss.

tiere, soprattutto negli aeroporti[84].

Rimandando per l'analisi sulle problematiche con la *privacy* alla letteratura di settore[85], l'attenzione va concentrata sulle implicazioni che l'impiego di tali strumenti ha sul principio di uguaglianza, in particolare con riferimento ad individui appartenenti a minoranze etniche.

Se, come visto, nell'ambito della gestione del fenomeno criminale la discriminazione dello straniero e del "diverso" sono storicamente attribuibili a fattori storico-sociali, nel campo del riconoscimento facciale e, più ampiamente, dell'elaborazione delle immagini, esiste un ulteriore fattore, di tipo tecnico-strutturale, che ha contribuito alla creazione e perpetuazione di distorsioni e *bias* pregiudizievoli per le minoranze. Fin dal XIX secolo, infatti, le caratteristiche fisiche dei reagenti chimici fotosensibili nelle prime macchine fotografiche, nonché le tecniche di sviluppo delle relative pellicole, risultavano più adatte a rappresentare soggetti dalla pelle chiara[86]. Le soluzioni videofotografiche, di conseguenza, vengono da sempre progettate al fine di ottenere risultati ottimali per individui con caratteristiche somatiche specifiche, come appunto la pelle chiara, lasciando così i soggetti che si discostano da tale *standard* (persone con pelle scura) vulnerabili a errori e distorsioni nei risultati. È naturale, di tal guisa, che anche le tecnologie di riconoscimento facciale riportino e perpetuino le medesime distorsioni. Esse, infatti, compiono calcoli di tipo probabilistico con una percentuale variabile di errore influenzata da molteplici fattori, come la qualità e la risoluzione dell'immagine, l'eventuale riflesso della luce, l'ambiente ove l'immagine viene acquisita, i movimenti del

[84] BERNAL, *AI Lie detectors to be tested by the Eu at border points*, in *The Telegraph*, 1 novembre 2018.

[85] Come già anticipato, infatti, l'intenzione del presente contributo è quella di analizzare le distorsioni in termini di uguaglianza, ma sono innumerevoli i problemi legati all'utilizzo in ambito pubblico dei citati sistemi di sorveglianza. Solo alcune delle complicanze possono rintracciarsi nell'incompatibilità con il diritto alla vita privata tutelato dall'art. 17 del Patto internazionale sui diritti civili e politici, dall'art. 8 della Convenzione europea dei diritti dell'uomo e dall'art. 7 della Carta dei diritti fondamentali dell'Unione europea e con la libertà di movimento, di opinione e di espressione, tutelata dagli articoli 12 e 19 Patto internazionale, dall'art. 2 del protocollo 4 C.E.D.U. e dall'art. 10 C.E.D.U., artt. 11 e 45 Carta dei diritti fondamentali. Sul punto v. amplius, EUROPEAN AGENCY FOR FUNDAMENTAL RIGHST, cit.

[86] Sul punto v. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 218 e la bibliografia ivi citata, in particolare LEWIS, *The Racial Bias Built into Photography,* in *The New York Times*, 25 aprile 2019.

soggetto, la sua età, le condizioni della sua pelle ed anche, chiaramente, il colore di quest'ultima[87].

A ciò si aggiunge l'ulteriore fattore, già analizzato con riferimento agli algoritmi predittivi, relativo alla scarsa qualità e rappresentatività dei dati scelti per allenare gli algoritmi biometrici. Il più delle volte, infatti, le immagini che compongono il *training set* di un sistema di riconoscimento facciale sono raccolte in modo casuale dal *web* o dai *social network*, senza il consenso degli interessati o delle piattaforme stesse, ed in mancanza di qualsivoglia forma di attenzione alla rappresentatività e pluralità delle stesse, con la conseguenza che tali *set*, la maggior parte delle volte, riflettono direttamente le relazioni di potere e i privilegi delle realtà sociali rappresentate sul *web*[88].

Diversi studi[89] hanno dimostrato che gli algoritmi che regolano il funzionamento dei sistemi di riconoscimento facciale hanno percentuali di precisione fortemente variabili in base al soggetto analizzato. Gli abbinamenti errati ricadono, appunto, in modo sproporzionato sulle categorie minoritarie, come donne e persone di colore, rispetto alle quali si ottiene il maggior numero di falsi positivi[90]: mentre nel caso di uomini di carnagione chiara i *software* raggiungono una precisione del 99%, quando si analizzano i volti di donne o di persone di colore, le percentuali di precisione scendono drasticamente, arrivando al 35% per le donne di pelle scura[91]. I *dataset* utilizzati per alimentare ed allenare i sistemi di riconoscimento, sarebbero infatti composti per l'80 % da immagini di individui dalla pelle chiara, e per il 75% da soggetti di sesso maschile.

Da tale mancanza di rappresentatività deriva inevitabilmente una forte difficoltà per il sistema di riconoscimento facciale ad individuare con un sufficien-

---

[87] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 32.

[88] *Ibid.*, 222.

[89] LOHR, *Facial Recognition is Accurate, if You're a White Guy*, in *The New York Times*, 9 febbraio 2018; GROTHER-NGAN-HANAOKA, *Face Recognition Vendor Test*, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, 2019.

[90] JOH, *Ethical AI in American Policing*, cit., 263; HARMON, *As Cameras Track Detroits Residents, A Debate Ensues Over Racial Bias. Part I*, in *The New York Times*, 8 luglio 2019.

[91] BOULAMWINI-GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning Research*, 2018, 9; AHMED, *Uk Passport photo checker shows bias against dark-skinned women*, in *BBC News*, 8 ottobre 2020.

te grado di accuratezza persone che differiscano dal caso "*standard*" (uomo bianco), con rischi di discriminazione elevatissimi soprattutto per asiatici ed afroamericani, che avrebbero una probabilità da 10 a 100 volte più elevata di essere identificati erroneamente rispetto ai bianchi[92]. Anche i sistemi di *emotion-detection* disvelano le medesime difficoltà nel cogliere con sufficiente accuratezza le particolarità di volti diversi dall'uomo caucasico; si pensi, ad esempio, al particolare taglio degli occhi delle persone asiatiche, che alcuni *software* hanno scambiato per un occhiolino o per lo strizzo degli occhi tipico del sorriso[93].

Se già, quindi, l'utilizzo di tali sistemi in campo privato solleva dubbi con riferimento al rispetto dei diritti fondamentali, l'impiego da parte della autorità di *law enforcement* può comportare effetti disastrosi[94].

4. *Intelligenza artificiale e controllo delle frontiere.* Chiarita la correlazione tecnica tra impiego di sistemi di intelligenza artificiale ed effetti discriminatori, occorre ora soffermarsi sulle relative ricadute applicative nell'ambito del controllo delle frontiere, nonché sulle modalità attraverso cui le distorsioni che ne derivano si riverberano, per effetto dell'interoperabilità dei *software* impiegati e dei correlativi *database*, anche sul piano della giustizia penale e della prevenzione dei reati.

La regolamentazione legislativa dell'immigrazione e, più in generale, del trattamento dello straniero entro e oltre i confini statali costituisce materia delicata, da sempre caratterizzata dalla necessità di un costante bilanciamento tra diversi interessi: da un lato le esigenze solidaristiche e umanitarie e, dall'altro, le pressanti ragioni di sicurezza e ordine pubblico[95]. Materia, quindi, in cui si annida il rischio di violazioni sistematiche dei diritti fondamentali dei soggetti

[92] GROTHER-NGAN-HANAOKA, *Face Recognition Vendor Test (FVRT). Part 3: Demographic Effects,* NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, 2019.
[93] SHARP, *Nikon Camera Says Asians are Always Blinking*, in *The Society Pages*, 29 maggio 2009.
[94] Per alcuni esempi di arresti basati su riconoscimenti erronei, v. HILL, *Wrongfully Accused by an Algorithm*, in *The New York Times*, 24 giugno 2020; HILL, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, in *The New York Times,* 29 dicembre 2021; HOGGINS, *'Racist and sexist' facial recognition cameras could lead to false arrests,* in *The Telegraph*, 20 dicembre 2019; ANDERSON, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He didn't Commit*, in *Detroit Free Press*, 12 luglio 2020.
[95] MORSELLI, *Diritto e Procedura penale dell'immigrazione*, Napoli, 2012, 6.

coinvolti, spesso vulnerabili e in fuga da povertà e guerre[96].
Certamente, ove si osservino le legislazioni nel tempo succedutesi nel nostro Paese sin dalla Legge Martelli[97], pare che la spinta securitaria e le istanze di difesa sociale abbiano avuto la meglio sulle esigenze di legalità e che «la breccia dell'emergenza (sia) stata la cifra preponderante nei cui allarmistici confini le scelte normative si sono affastellate»[98].
La paura verso lo straniero ha sicuramente origini antichissime e poggia le proprie solide basi sull'identificazione «extracomunitario uguale criminale»[99], clandestino "fuori legge" e quindi fuorilegge, che delinque[100]. La società occidentale, sostanzialmente compatta nella paura dei migranti[101], indifferentemente dalle divergenze politiche e ideologiche, ha eretto una barriera invalicabile tra cittadini e stranieri[102], contribuendo ad un razzismo «istituzionale»[103] e ad una vera e propria lotta sociale all'invasione migratoria, da combattere con gli strumenti dell'ordine pubblico[104] e con misure sempre più repressivo-segregazionistiche[105].
Proprio tale spinta securitaria, come accennato nell'introduzione[106], ha contribuito alla nascita del fenomeno della "*crimmigration*", definibile come la sovrapposizione (che a volte diventa fusione) tra diritto dell'immigrazione e diritto penale[107] che, secondo una tripartizione offerta da attenta dottrina[108], si svi-

[96] Così GATTA, *La pena nell'era della 'crimmigration': tra Europa e Stati Uniti*, cit., 989.
[97] L. 28 febbraio 1990, n. 39.
[98] DI CHIARA, *"Due occhi scuri". Immigrazione, diritti fondamentali e lessico fraterno: tracce per un postludio*, in VERDE-GENNA, *Immigrazione e garanzie dei diritti fondamentali,* Palermo, 2012, 424.
[99] LO MONTE, *Il fenomeno dell'immigrazione clandestina: diritti, sicurezza e criminalità*, cit., 145.
[100] DAL LAGO, *Non-persone. L'esclusione dei migranti in una società globale,* cit., 49.
[101] Per un'interessante riflessione sulla "massificazione" degli immigrati e la connessa paura dell'invasione di massa, più che del singolo immigrato, v. SPENA, *La crimmigration e l'espulsione dello straniero-massa*, cit., 502 ss.
[102] DAL LAGO, *Non-persone. L'esclusione dei migranti in una società globale,* cit., 43.
[103] FERRAJOLI, *La criminalizzazione degli immigrati (note a margine alla legge 94.2009),* in *Quest. Giust.,* 2009, 5, 17.
[104] Così CRUPI, *Diritto penale d'autore, diritto penale del nemico e diritto penale del fatto: quale modello per la posizione dello straniero?,* in VERDE-GENNA, *Immigrazione e garanzie dei diritti fondamentali,* cit., 288.
[105] CAPUTO, *I reati collegati all'espulsione: profili generali e principali questioni applicative*, in *Dir. pen. proc,* 2009, Speciale 1, 9 ss.
[106] V. *infra*, par. 1, 4.
[107] GATTA, *La pena nell'era della 'crimmigration': tra Europa e Stati Uniti*, cit., 992.
[108] *Ibid.,* 990 ss.

lupperebbe lungo tre diverse fenomenologie: la previsione di conseguenze penali per la violazione di norme di diritto dell'immigrazione; la previsione di conseguenze rilevanti sul piano del diritto dell'immigrazione derivanti da condanne penali; il ricorso a misure privative della libertà personale nell'ambito del diritto dell'immigrazione. Già solamente osservando le numerose fattispecie penali contenute nel nostro Testo unico sull'immigrazione, può aversi contezza del fenomeno. Eppure, trattasi di materia ampiamente disciplinata già a livello amministrativo, con la previsione di sanzioni anche molto severe per tutti gli illeciti rilevanti sul piano penale. La predisposizione di misure penali, a tal riguardo, pare essere tanto inutile quando socialmente percepita come necessaria, in un'ottica di collettiva disapprovazione sociale dell'immigrazione clandestina a cui il Parlamento, indipendentemente dal colore politico della maggioranza, sceglie di rispondere simbolicamente con tale strumento[109].

Trattasi di un fenomeno descritto anche come neocolonialismo punitivo, consistente nell'atteggiarsi del diritto penale e dell'esercizio del potere di punire in modo diverso nei confronti di coloro che vengono concepiti come "altri" rispetto al destinatario *standard*, in continuità con le pratiche punitive proprie, appunto, del diritto penale coloniale[110].

È quindi alla luce del descritto quadro che occorre, in questa sede, interrogarsi su quale sia il ruolo dell'intelligenza artificiale e su come l'impiego delle nuove tecnologie in questo ambito possa contribuire all'ulteriore criminalizzazione dei migranti, comportando rischi per la già precaria tutela dei loro diritti fondamentali.

La materia del controllo dei flussi migratori, infatti, si orienta sempre più verso la fusione tra tre direttrici: *criminalization* e *securitization*, di cui il diritto

[109] *Ibid.,* 995.

[110] Per un'attenta analisi del fenomeno v. RICCI, *Alterità e potere punitivo nello scenario europeo e contemporaneo. Spunti a sostegno di un approccio critico post-coloniale*, in *www.legislazionepenale.eu,* 1 dicembre 2022. Secondo l'Autrice «piuttosto che dinanzi a un'Europa veramente post-moderna, dove dovrebbe dominare l'idea del rispetto e della tutela delle differenze (ovvero dell'alterità in senso positivo), ci troviamo di fronte a un'Europa "modernista" che, lungi dal rappresentare il superamento dello Stato-nazione, ne diviene una nuova, definitiva riaffermazione» e «il punire, operando in maniera massiccia e su più fronti sempre allo scopo di rafforzare l'operatività della frontiera, imprime sui migranti un contrassegno di alterità, questa volta più direttamente associato all'idea di un'accentuata propensione al crimine da parte di costoro» (*Id.,* 12).

penale costituisce l'anima portante, e da ultimo, in funzione servente rispetto alle prime due*, technologization*[111]. La "fortezza Europa", protagonista di anni di politiche volte all'esclusione dei migranti irregolari e dei richiedenti asilo mediante il rafforzamento e la materializzazione dei confini e delle frontiere, ha cominciato a dotarsi di infrastrutture intelligenti per perseguire gli obiettivi di respingimento[112] e la *war against terror* ha costituito la leva principale per il superamento di confini meramente legali, prima considerati solidi e duraturi[113].

I profili critici delle intersezioni tra nuove tecnologie e controllo delle frontiere paiono essere principalmente due: a) le conseguenza discriminatorie, potenzialmente incidenti sulla libertà personale, derivanti dall'utilizzo di *risk assesment tools*, *emotion-dection tools* e tecnologie biometriche di vario genere in sede di respingimento dello straniero alla frontiera, di rilascio di visti e permessi o di decisioni inerenti la detenzione amministrativa pre-rimpatrio; b) l'inserimento dei dati personali dell'immigrato, rilevati al momento dell'ingresso nel territorio dello stato, in *database* che, in forza della loro interoperabilità, possono essere attinti dalle autorità statali per finalità di mantenimento dell'ordine e della sicurezza pubblica e di lotta alla criminalità.

Partendo dalla prima linea d'indagine, senza intenzione alcuna di soffermarsi sulla complessa disciplina dell'ingresso nello straniero in Italia, basti ricordare in questa sede che, dopo anni in cui la riserva di legge prevista dall'art. 10 Cost. in materia di condizione giuridica dello straniero è rimasta disattesa, è intervenuta a disciplinare la materia la L. 28 febbraio 1990, n. 39, seguita poi il dalla L. 6 marzo del 1998, n. 40, c.d. Turco-Napolitano, poi trasfusa nel Testo unico sull'immigrazione (d'ora in poi TUI) contenuto nel decreto legislativo 25 luglio 1998, n. 286. Il Testo unico, in conformità agli accordi di Schengen, ridisciplina la materia del controllo delle frontiere esterne, prevedendo due principali strumenti per impedire l'ingresso e il soggiorno irregola-

[111] DI MARTINO, *L'intervento penale in materia d'immigrazione e i suoi limiti (per un'introduzione),* in *Immigrazione illegale e diritto penale. Un approccio interdisciplinare*, a cura di Rosi-Rocchi, Napoli, 2013, 3 ss.

[112] BROEDERS, *The New Digital Borders of Europe. EU Databases and the Surveillance of Irregular Migrants,* in *International Sociology,* 2007, vol. 22, 1, 72.

[113] *Ibid.,* 78.

ri nel territorio italiano: il respingimento e l'espulsione.
Dopo aver previsto, al comma terzo dell'art. 4 che «Non è ammesso in Italia lo straniero che non soddisfi tali requisiti o che sia considerato una minaccia per l'ordine pubblico o la sicurezza dello Stato o di uno dei paesi con i quali l'Italia abbia sottoscritto accordi per la soppressione dei controlli alle frontiere interne e la libera circolazione delle persone [...]», l'art. 10 TUI, disciplinando specificamente il «respingimento», prevede che: «La polizia di frontiera respinge gli stranieri che si presentano ai valichi di frontiera senza avere i requisiti richiesti dal presente testo unico per l'ingresso nel territorio dello Stato» e che «Il respingimento con accompagnamento alla frontiera è altresì disposto dal questore nei confronti degli stranieri: a) che entrando nel territorio dello Stato sottraendosi ai controlli di frontiera, sono fermati all'ingresso o subito dopo; b) che, nelle circostanze di cui al comma 1, sono stati temporaneamente ammessi nel territorio per necessità di pubblico soccorso». Esistono quindi due tipi di respingimento, uno adottato dalla polizia di frontiera al momento della presentazione dello straniero al confine e uno dal questore, che gli attribuisce il potere di inseguire ed allontanare, in forma coattiva, gli stranieri già entrati nel territorio senza sottoporsi ai controlli di frontiera.
Per quanto riguarda l'espulsione, il TUI ne prevede tre tipologie: una amministrativa, una come misura di sicurezza e una come sanzione sostitutiva della detenzione. Soffermandoci sulla prima, l'art. 13 prevede che lo straniero venga espulso dal territorio nazionale: a) per motivi di ordine pubblico o di sicurezza; b) per essere entrato nel territorio in modo clandestino e quindi senza sottoporsi ai controlli; c) per presenza irregolare sul territorio; d) per sospetta pericolosità sociale. L'esecuzione del provvedimento amministrativo di espulsione può avvenire mediante accompagnamento immediato alla frontiera a mezzo della forza pubblica oppure mediante intimazione a lasciare il territorio. L'art. 14 TUI prevede poi che, ove non sia possibile eseguire con immediatezza l'espulsione mediante accompagnamento o respingimento, il questore disponga il trattenimento «per il tempo strettamente necessario» presso un centro di permanenza per i rimpatri (d'ora in poi CPR), disposto con priorità nei confronti degli stranieri considerati una minaccia per l'ordine e la sicurezza pubblica o condannati per alcuni gravi reati.

I CPR, oggetto di accesissimo dibattito, soprattutto con riguardo alla loro natura giuridica di sanzione sostanzialmente penale[114], "ospitano" quindi i migranti in situazioni di irregolarità rispetto alle norme concernenti l'ingresso e il soggiorno. L'attuale Testo di riferimento in materia è da individuarsi nella Direttiva Rimpatri (la n. 2008/115/CE), anche se in Italia è stata la L. 6 marzo 1998, n. 40, c.d. Turco-Napolitano, ad averli istituiti per la prima volta, prevedendo un tempo massimo di trattenimento pari a 30 giorni, esteso poi ad opera di successivi interventi legislativi.

Tali centri, seppur assimilabili, *de facto*, a istituti penitenziari, risultano privi di una regolamentazione organica che disciplini il rispetto dei diritti dei trattenuti ed anche la loro gestione, che rientra nelle competenze delle Prefetture, viene affidata ad enti attuatori attraverso bandi pubblici, risultando quindi estremamente disomogenea a livello territoriale.

Orbene, le legislazioni di moltissimi paesi occidentali contengono disposizioni assimilabili a quelle appena citate, prevedendo, innanzitutto, un necessario vaglio sulla "affidabilità" dello straniero che intende valicare i confini del Paese eventualmente ospitante e, poi, il trattenimento presso appositi centri di coloro che si trovino in situazione di irregolarità[115].

È fatto noto che, sin dall'entrata in vigore del Trattato di Amsterdam e dall'introduzione nel Trattato costitutivo CE dell'art. 63, nell'ottica della piena realizzazione dello spazio di libera circolazione europeo, anche la materia dell'immigrazione e la disciplina dei visti e dell'asilo ha smesso di essere appannaggio esclusivo degli Stati per essere regolamentata a livello comunitario, sì da gradualmente omogeneizzare le regole vigenti nel territorio dell'Unione.

Secondo i dati dell'Eurostat, in particolare le *Statistics on enforcement of*

---

[114] Sul punto v., tra gli altri, GATTA, *La pena nell'era della 'crimmigration': tra Europa e Stati Uniti*, cit., 1010 ss.; DI MARTINO-BIONDI DAL MONTE-BOIANO-RAFFAELLI, *The criminalization of irregular immigration: law and practice in Italy*, cit., 108 ss.; PISA, *La repressione dell'immigrazione irregolare: un'espansione incontrollato della normativa penale?,* in *Dir. pen. proc.,* 2019, Speciale 1, 5 ss.; MASERA, *I centri di detenzione amministrativa cambiano nome ed aumentano di numero, e gli hotspot rimangono privi di base legale: le sconfortanti novità del Decreto Minniti*, in *Dir. Pen. Cont.*, 2017, 3, 278 ss.; DONINI, *Il cittadino extracomunitario da oggetto materiale a tipo d'autore nel controllo penale dell'immigrazione,* cit., 127 ss.

[115] Ad esempio, in Spagna il Real Decreto 1155/2024, de 19 de noviembre, Capitulo II; in Germania l'**Aufenthaltsgesetz (AufenthG), § 15; in Francia** *Code de l'entrée et du séjour des étrangers et du droit d'asile*, art. L332-1.

immigration legislation, nel 2023 gli Stati membri hanno negato l'ingresso nel territorio dell'Unione a 118.935 persone tra respingimenti via mare, alle frontiere terresti o negli aeroporti[116].

Ed è proprio nella gestione dei respingimenti, delle espulsioni e delle relative modalità esecutive mediante detenzione amministrativa che, negli ultimi anni, l'uso dell'intelligenza artificiale si è prepotentemente imposto, divenendo pratica invalsa. A tal riguardo, gli esperti hanno utilmente coniato il termine «confini digitali»[117] o *tecnoborders*, per parlare di confini la cui infrastruttura si basa sempre più su *machine learning, big data* e sistemi di decisione automatizzata. Numerose sono, infatti, le occasioni in cui, agli operatori pubblici preposti al controllo delle frontiere, è richiesto di formulare valutazioni individualizzate nei confronti del cittadino straniero, pur in presenza di un quadro informativo personale fortemente lacunoso. Tali giudizi riguardano, ad esempio, come desumibile dalle citate disposizioni del TUI, la potenziale pericolosità dello straniero per la sicurezza pubblica, la sussistenza di requisiti per l'ingresso o la permanenza nel territorio statale, la necessità di trattenimento in un CPR, o la presumibile osservanza dell'ordine di espulsione. Proprio al fine di supportare tali decisioni si è quindi progressivamente fatto ricorso – in particolare nell'ambito dell'Unione europea, ma anche in contesti extraeuropei – a strumenti tecnologici, presentati come soluzioni ottimali per sopperire all'incertezza informativa ed aumentare l'efficienza e la celerità decisionale[118].

A livello empirico, un primo fenomeno osservabile e decisamente preoccupante è sicuramente l'impiego di tecnologie biometriche nel processo di valutazione delle richieste di asilo o di visto; pratica, questa, che solleva non poche preoccupazioni relativamente alla possibilità di discriminazioni, dirette o indirette, basate sulla razza, l'etnia o l'origine nazionale dei soggetti coinvolti.

---

[116] Consultabile al link *https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Enforcement_of_immigration_legislation_statistics*.

[117] BROEDERS, *The New Digital Borders of Europe. EU Databases and the Surveillance of Irregular Migrants,* in *International Sociology,* cit., 71 ss.

[118] Sul punto cfr. AMNESTY INTERNATIONAL, *Primer: Defending the rights of refugees and migrants in the digital age*, 2024; RELATORE SPECIALE DELLE NAZIONI UNITE SULLE FORME CONTEMPORANEE DI RAZZISMO, DISCRIMINAZIONE RAZZIALE, XENOFOBIA E INTOLLERANZA, *Racial Discrimination and emerging technologies,* Documento ONU n. A/HRC/44/57, 18 giugno 2020.

In particolare, nell'ottobre 2018, l'Unione europea ha annunciato il finanziamento di un progetto denominato IBorderCTRL, un sistema automatizzato del controllo dei confini (ad oggi non ancora reso operativo), che è stato finanziato con 4,5 milioni di euro dal programma di ricerca della Commissione europea Horizon 2020 e sperimentato negli aeroporti di alcuni dei paesi dell'Unione dal settembre 2016 all'agosto 2019 (in particolare in Grecia, Ungheria e Lettonia). Questo sistema utilizza l'intelligenza artificiale, mediante l'analisi dei movimenti facciali, per individuare le menzogne durante un quiz che viene tenuto da una guardia di frontiera virtuale a coloro che vogliono entrare nel territorio dello stato, analizzandone le espressioni facciali mediante sistemi di riconoscimento e categorizzazione biometrica. I viaggiatori che, secondo il sistema, rispondono onestamente possono attraversare la frontiera, mentre gli altri vengono indirizzate alle guardie umane per ulteriori controlli.
Non vi è dubbio sul fatto che tale proposta sollevi gravi problematiche di natura etica, soprattutto avendo presenti le già viste e numerosissime fallacie dei sistemi di riconoscimento delle emozioni e dei tratti del viso ove utilizzati su soggetti diversi dal caso *standard* (uomo bianco). Il rischio di incorrere in misinterpretazioni di indicatori culturali non assimilabili a quelli su cui l'algoritmo si è allenato sarebbe elevatissimo, tralasciando la dimostrata erroneità (o, perlomeno, altissima problematicità) delle teorie su cui si basa, in generale, la scienza del rilevamento della verità mediante l'analisi delle micro-espressioni facciali[119].
Sempre a livello eurounitario è stato testato un altro *software*, il Sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), anch'esso non attualmente operativo, che si interfaccia con dati disponibili pubblicamente *online*, per determinare la minaccia che un viaggiatore, che si reca nello spazio Schengen senza visto, potrebbe rappresentare per la sicurezza dell'Europa. Anche qui, le conseguenze pregiudizievoli si abbatterebbero con maggior forza su alcune categorie di individui, che l'algoritmo potrebbe "statisticamente" considerare pericolosi perché, ad esempio, provenienti da paesi arabi e quin-

[119] Sul punto v. FELDMAN BARRETT-ADOLPHS-MARSELLA-MARTINEZ-POLLAK, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, in *Psychol Sci Public Interest,* 20 luglio 2019.

di associati a minacce di terrorismo. La categorizzazione automatica degli individui sulla base di informazioni superficiali, come quelle reperibili sul *web,* ne comporterebbe inevitabilmente una forte "razzializzazione", con conseguenze preoccupanti in tema di marginalizzazione e criminalizzazione etnicamente orientata di intere fasce di popolazione.

Anche singoli Stati, per lo più extra-europei (come Canada[120] e Regno Unito[121]) hanno testato o persino previsto regolarmente, a sostegno della decisione degli operatori degli uffici immigrazione per il rilascio dei visti di ingresso o dell'accoglimento delle domande di asilo, algoritmi predittivi basati su *risk assesment* individuali. Tali tecnologie – suscettibili, come visto, a *bias*, errori sistemici e malfunzionamenti – hanno, come prevedibile, comportato conseguenze sproporzionate per determinate categorie di persone, causando espulsioni e rigetti pressoché arbitrari[122].

Per quanto riguarda l'Europa, un esempio può essere rinvenuto in Germania ove, sin dal 2017, viene utilizzato un sistema di riconoscimento dialettale (*Dialect Identification Assistance System,* DIAS) nell'ambito dell'istruttoria delle domande di protezione internazionale[123]. L'obiettivo dichiarato dell'impiego di tale tecnologia è quello di coadiuvare le autorità nell'accertamento dell'attendibilità delle dichiarazioni dei richiedenti in merito alla propria provenienza geografica. Il funzionamento del sistema prevede la registrazione, da parte del richiedente asilo, di un messaggio vocale di circa due minuti, in cui questi è invitato a descrivere un'immagine nella lingua madre. I dati vocali vengono quindi elaborati dall'algoritmo, il quale produce una stima percentuale della somiglianza tra l'accento del parlante e una determinata varietà dialettale. Nonostante la natura ausiliaria che formalmente caratterizza il DIAS, l'esito fornito da tale strumento è stato spesso utilizzato quale elemento decisivo nella valutazione finale della domanda di asilo, solle-

[120] Sul punto v. MOLNAR-GILL, *Bots at the gate. A human rights analysis of automated decision-making in canadaìs immigration and refugee system,* Toronto, 2018.

[121] Nel Regno Unito il *visa streaming algorithm* veniva utilizzato per filtrare le richieste di visto fino al 2020, quando il Governo ne ha annunciato il ritiro a causa dei *bias* e dei conseguenti risultati discriminatori.

[122] AMNESTY INTERNATIONAL, *Primer*, cit., 19.

[123] ALGORITHM WATCH, *Automating Society Report*, 2020, (Germany section), consultabile su https://automatingsociety.algorithmwatch.org/report2020/germany/.

vando rilevanti preoccupazioni[124].

Passando alla seconda area di interesse, ovvero quella relativa all'interoperabilità dei *database* operanti in materia di gestione dei flussi migratori, giova premettere che le problematiche di cui ci si accinge a parlare rilevano in particolar modo nei confronti dell'immigrato irregolare che abbia già fatto ingresso nello Stato. Sul punto, è importante evidenziare che lo stato di "irregolarità" dello straniero può derivare da molteplici fattori ed essere originario (quindi corrispondente ad un ingresso irregolare) oppure derivato, ad esempio nel caso in cui un soggetto sia entrato legalmente nel territorio dello Stato per poi non uscirne allo scadere del proprio visto, oppure nel caso in cui un soggetto diventi destinatario di provvedimenti penali cui consegua l'espulsione. A tal riguardo le sole politiche di respingimento alla frontiera sono state ritenute insufficienti a garantire un'efficace lotta all'immigrazione irregolare, necessitando il supporto di sistemi operativi attivabili anche in un momento successivo all'ingresso del migrante[125]. L'uso di sistemi di "sorveglianza attiva" nel territorio degli Stati membri, finalizzata all'individuazione e successiva esclusione dallo Stato del migrante irregolare, necessita tuttavia di una grande mole di informazioni, che vengono recepite proprio grazie a tale interoperabilità, che riguarda principalmente dati biometrici.

Ai sensi del Regolamento (UE) 26 giugno 2013, n. 603 (*Regolamento Eurodac*), infatti, gli Stati membri dell'Unione europea hanno l'obbligo di procedere al rilevamento delle impronte digitali di tutti i cittadini di paesi terzi e degli apolidi di età pari o superiore a 14 anni che presentano domanda di protezione internazionale, nonché di coloro che vengono sorpresi nell'atto di attraversare irregolarmente una frontiera esterna dell'Unione. Inoltre, il medesimo Regolamento consente agli Stati membri di procedere alla rilevazione delle impronte digitali dei cittadini di paesi terzi rinvenuti in situazione di soggiorno irregolare nel territorio nazionale. In tale contesto, il concetto di interoperabilità dei dati – secondo una definizione proposta da Amnesty International – si riferisce a «l'abilità di un sistema o database di scambiare o reperire

[124] *Ibid.*

[125] BROEDERS, *The New Digital Borders of Europe. EU Databases and the Surveillance of Irregular Migrants,* in *International Sociology,* vol. 22(1), 2007, 73.

facilmente informazioni all'interno di un altro sistema o database»[126], determinando una grande estensione dell'utilizzo dei dati biometrici oltre la finalità originaria per cui sono stati raccolti e favorendone la condivisione tra autorità nazionali, agenzie di pubblica sicurezza e organizzazioni umanitarie.
In materia, il Regolamento UE 13 marzo 2024, n. 903 sull'interoperabilità[127] segna un passo cruciale nella strategia dell'Unione europea per la connessione e l'integrazione dei numerosi sistemi attualmente operanti nell'Unione stessa. Ci si riferisce, innanzitutto, al Sistema di informazione Schengen (d'ora in poi SIS), istituito contestualmente all'adozione della *Convenzione Schengen* ma che, a causa soprattutto dell'aumento del fenomeno terroristico nei primi anni 2000, da strumento originariamente ideato per il controllo delle frontiere mediante informazioni di tipo alfanumerico, si è lentamente trasformato in un sistema tecnologico volto ad effettuare indagini a tutela della sicurezza interna, con un database di dati biometrici e fotografie e la capacità di effettuare identificazioni anche in tempo reale[128]. Trattasi, appunto, di un sistema di sorveglianza basato su dati, composto da un *database* centrale situato a Strasburgo e da basi nazionali in tutti gli Stati membri. Le informazioni registrate dal sistema includono dati come nome, nazionalità, caratteristiche fisiche, ma anche eventuali valutazioni di pericolosità. Il SIS è affiancato da SIRENE, un sistema supplementare, che facilita lo scambio di informazioni complementari, come impronte digitali e fotografie. Nel 2007, lo sviluppo di un sistema di seconda generazione, SIS II, ha marcato definitivamente il carattere dello stesso da strumento di controllo delle frontiere a strumento di indagine a tutela della sicurezza interna, accrescendo la possibilità di accesso ai relativi dati da parte delle autorità pubbliche[129]. Il sistema è ora disciplinato da tre diversi regolamenti, di cui uno, significativamente, operante nel settore della cooperazione di polizia e giudiziaria in ambito penale[130].

---

[126] AMNESTY INTERNATIONAL, *Primer*, cit., 7.
[127] Regolamento (UE) 2024/903 del Parlamento europeo e del Consiglio del 13 marzo 2024 che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione.
[128] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 252.
[129] *Ibid.*
[130] Regolamento (UE) 2018/1862 del 28 novembre 2018 sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen nel settore della cooperazione di polizia e della cooperazione giudiziaria in ma-

Altro *database* di fondamentale importanza è quello dell'EES (*Entry/Exit System*), che consente di registrare digitalmente l'ingresso e l'uscita dei cittadini di paesi terzi che entrino nello spazio Schengen per periodi di breve durata, generando degli avvisi automatici verso gli Stati membri alla scadenza del periodo previsto. In determinate situazioni, il sistema può essere utilizzato con finalità di *law enforcement*, come la lotta al terrorismo o altri crimini gravi[131].
Merita segnalazione, poi, l'Eurodac (*European Dactylographic*), *database* europeo delle impronte digitali per coloro che richiedono asilo[132], ideato al fine di contrastare il fenomeno del "*asylum shopping*" e permettere agli Stati membri di sapere se un soggetto richiedente abbia già presentato domanda altrove. A tale limitata categoria di soggetti schedati è stata poi aggiunta quella degli immigrati irregolari di cui fosse impossibile risalire all'identificazione, sorpresi ad attraversare illegalmente i confini oppure trovati sul territorio dello Stato senza titolo. A tal riguardo, nel maggio del 2024 il Parlamento europeo ha firmato un Patto su migrazione e asilo, contenente ben dieci testi legislativi[133] che riformano la politica europea di migrazione asilo, tra cui anche la

---

teria penale che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione.

[131] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 265.

[132] EUROPEAN COMMISSION, *Proposal for a Regulation on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of Regulation Eu n. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application from international protection lodged in one of The Member States by a third-country national o a state-less person, for identifying an illegal staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes* (recat), COM(2016)0272 – 2016 (COD), 4 maggio 2016.

[133] Regolamento (UE) 2024/1347 del Parlamento europeo e del Consiglio, del 14 maggio 2024, recante norme sull'attribuzione a cittadini di paesi terzi o apolidi della qualifica di beneficiario di protezione internazionale, su uno *status* uniforme per i rifugiati o per le persone aventi titolo a beneficiare della protezione sussidiaria e sul contenuto della protezione riconosciuta, che modifica la direttiva 2003/109/CE del Consiglio e che abroga la direttiva 2011/95/UE del Parlamento europeo e del Consiglio; Regolamento (UE) 2024/1348 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che stabilisce una procedura comune di protezione internazionale nell'Unione e abroga la direttiva 2013/32/UE; Direttiva (UE) 2024/1346 del Parlamento europeo e del Consiglio, del 14 maggio 2024, recante norme relative all'accoglienza dei richiedenti protezione internazionale Regolamento (UE) 2024/1351 del Parlamento europeo e del Consiglio, del 14 maggio 2024, sulla gestione dell'asilo e della migrazione, che modifica i regolamenti (UE) 2021/1147 e (UE) 2021/1060 e che abroga il regolamento (UE) n. 604/2013 Regolamento (UE) 2024/1358 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che istituisce l'«Eurodac» per il confronto dei dati biometrici ai fini dell'applicazione efficace dei regolamenti (UE)

revisione del sistema Eurodac. Tra le innovazioni più rilevanti vi è l'abbassamento dell'età minima per il rilevamento dei dati biometrici a sei anni, nonché l'estensione dell'ambito dei dati raccolti, che ora include anche le immagini facciali. Anche questo strumento, grazie all'ampliamento delle sue iniziali funzioni, ricomprende adesso scopi legati alle politiche di sicurezza.

Va menzionato, infine, il Sistema di informazione visti, (VIS) posto a presidio dei controlli delle frontiere dello spazio Schengen, che registra i dati di tutti coloro che entrano nei paesi Schengen con visto. Il sistema è stato concepito all'indomani dell'11 settembre 2001 e presenta una forte connotazione antiterroristica[134], ponendosi sulla scia della generale tendenza alla graduale assimilazione, dopo i fatti del 2001, tra misure antimmigrazione e misure antiterrorismo, che ha portato alla costruzione di una «ingegneria sociale coercitiva» verso gli stranieri[135], ove la lotta al terrorismo viene condotta tanto sul piano della giustizia penale che su quello del diritto dell'immigrazione, con il relativo apparato di *enforcement*[136].

È proprio a seguito degli attacchi terroristici del 2015 e 2016 in Francia e Bel-

---

2024/1351 e (UE) 2024/1350 o del Parlamento europeo e del Consiglio e della direttiva 2001/55/CE del Consiglio e ai fini dell'identificazione dei cittadini di paesi terzi e apolidi il cui soggiorno è irregolare, e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, che modifica i regolamenti (UE) 2018/1240 e (UE) 2019/818 del Parlamento europeo e del Consiglio e che abroga il regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, Regolamento (UE) 2024/1349 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che stabilisce una procedura di rimpatrio alla frontiera e che modifica il regolamento (UE) 2021/1148 Regolamento (UE) 2024/1352 del Parlamento europeo e del Consiglio, del 14 maggio 2024, recante modifica dei regolamenti (UE) 2019/816 e (UE) 2019/818, allo scopo di introdurre accertamenti nei confronti dei cittadini di paesi terzi alle frontiere esterne, Regolamento (UE) 2024/1356 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che introduce accertamenti nei confronti dei cittadini di paesi terzi alle frontiere esterne e modifica i regolamenti (CE) n. 767/2008, (UE) 2017/2226, (UE) 2018/1240 e (UE) 2019/817, Regolamento (UE) 2024/1359 del Parlamento europeo e del Consiglio, del 14 maggio 2024, concernente le situazioni di crisi e di forza maggiore nel settore della migrazione e dell'asilo e che modifica il regolamento (UE) 2021/1147, Regolamento (UE) 2024/1350 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che istituisce un quadro dell'Unione per il reinsediamento e l'ammissione umanitaria e modifica il regolamento (UE). I regolamenti si applicheranno dal giugno 2026.

[134] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 261.

[135] MILLER, *Blurring the Boundaries Between Immigration and Crime Control after Sept. 11th*, in *25 B.C. Third World Law Journal*, 2005, 95.

[136] GATTA, *La pena nell'era della 'crimmigration': tra Europa e Stati Uniti*, cit., 1002.

gio, infatti, che la Commissione europea ha formulato una proposta di Regolamento[137] volta ad ampliare le funzionalità del VIS, estendendone gli scopi alla prevenzione delle minacce alla sicurezza interna.

Orbene, il Regolamento sull'interoperabilità prevede l'integrazione di questi sistemi in una struttura centralizzata composta da diverse piattaforme: un Portale di ricerca europeo (ESP) che consente a tutte le autorità in possesso dell'autorizzazione all'accesso ad uno dei sistemi interconnessi di effettuare ricerche ad ampio raggio su tutti i relativi *database*; un sistema di *Biometric Matching* condiviso, in grado di conservare i profili biometrici contenuti nei sistemi interconnessi; un deposito centrale contenente *file* individuali con informazioni personali dei soggetti registrati; un *Multiple Identity Detector* in grado di memorizzare i collegamenti tra i vari *database* ed estrarne informazioni utili.

Si registra, quindi, relativamente a tutti i sistemi inizialmente ideati per l'ordinata gestione dei flussi migratori, un graduale incremento di funzionalità (in ambito tecnologico definibile come *function creep*) a beneficio delle forze dell'ordine, che ne ha lentamente snaturato lo scopo iniziale, sollevando anche delicate problematiche giuridiche[138].

Questo ampliamento, insieme all'allargamento delle possibilità di accesso da parte delle autorità nazionali, segna infatti un passaggio verso forme di sorveglianza digitale sistemica, che trasformano il corpo del migrante in un vettore di identificazione permanente, assimilabile a un passaporto biometrico, rievocando pratiche di catalogazione proprie del passato coloniale. In tal modo, la riforma si configura quale dispositivo tecnico a sostegno di un approccio securitario e coercitivo alla mobilità umana, fondato su dinamiche di criminalizzazione, detenzione e rimpatrio forzato[139]. Il risultato finale, frutto di anni di

[137] Che ha portato poi all'adozione del Regolamento (UE) 2021/1134 del Parlamento europeo e del Consiglio, del 7 luglio 2021, che modifica i regolamenti (CE) n. 767/2008, (CE) n. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 e (EU) 2019/1896 del Parlamento europeo e del Consiglio e che abroga le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, ai fini della riforma del sistema di informazione visti.

[138] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 249.

[139] LANGUAGE AID, *Le Popolazioni migranti nell'epoca dell'intelligenza artificiale, Scheda di approfondimento 2, 3,* consultabile su *https://www.meltingpot.org/2024/09/le-popolazioni-migranti-nellepoca-dellintelligenza-artificiale/.*

emergenze terroristiche, ha contribuito alla definitiva confusione, nello spazio europeo, tra gestione dell'immigrazione e contrasto al crimine e al terrorismo[140].

Come noto, le "finalità di pubblica sicurezza" e "l'ordine pubblico" costituiscono spesso la base per giustificare importanti eccezioni alla tutela dei diritti fondamentali. In tema di trattamento dei dati personali, ad esempio, il GDPR, La Convenzione europea dei diritti dell'uomo e la Direttiva 27 aprile 2016, n. 680 legittimano restrizioni alla *privacy* e alla protezione dei dati proprio quando ciò sia necessario per esigenza di sicurezza pubblica. Si tratta, in definitiva, della trasposizione della gestione del migrante dal piano della mobilità internazionale a quello della lotta al terrorismo, ambito in cui le autorità pubbliche godono di un ampio margine di discrezionalità ed il rischio di detrimento dei diritti fondamentali si fa più alto.

Un esempio dei rischi legati alla descritta interoperabilità può rinvenirsi già nel nostro ordinamento. L'art.10-*ter* TUI prevede, infatti, che lo straniero irregolare sia sottoposto, dopo l'ingresso nel territorio nazionale, a rilievi fotodattiloscopici. Tale obiettivo viene perseguito mediante il sistema degli *hotspots,* centri di accoglienza in cui il soggetto viene sottoposto allo *screening* sanitario, all'identificazione, alla registrazione e al fotosegnalamento entro 48 ore dal suo ingresso, a cui seguirà la sua classificazione in base alla relativa situazione giuridica: i richiedenti asilo saranno trasferiti in appositi *hub*, mentre i non richiedenti protezione internazionale saranno spediti nei CPR, in attesa di essere espulsi[141].

Invero, i dati così rilevati vengono direttamente inseriti, oltre che nella banca dati Eurodac, anche nel Sistema automatizzato di identificazione delle impronte (AFIS)[142], da cui a sua volta attinge il SARI, ovvero il Sistema automatico di riconoscimento immagini utilizzato dalle forze di polizia italiane, sin dal 2017, ai fini di contrasto del terrorismo e della criminalità organizzata.

---

[140] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 250.

[141] MANGIARACINA, *Una "nuova" forma di detenzione per l'identificazione dei migranti*, in *Materiali per una storia della cultura giuridica*, 2017, 2, 589 ss.

[142] GARANTE NAZIONALE DEI DIRITTI DELLE PERSONE DETENUTE O PRIVATE DELLA LIBERTÀ PERSONALE, *Relazione al Parlamento*, 80.

Il *software*, le cui caratteristiche operative vengono spiegate nel capitolato tecnico allegato al contratto sottoscritto tra azienda fornitrice del sistema e Ministero dell'Interno[143], ha due funzionalità: SARI *Enterprise*, che permette di identificare un individuo mediante il confronto con le immagini contenute nella banca dati AFIS, e SARI *Real Time*, il cui compito è quello di confrontare in tempo reale i volti catturati dalle videocamere presenti su tutto il territorio nazionale ed emanare automaticamente un avviso quando viene trovata una corrispondenza tra persona ripresa e *database*, sì da fornire supporto alle forze dell'ordine in occasione, ad esempio, di manifestazioni pubbliche o situazioni di rischio[144]. In questa funzione, il programma, una volta inserito il *frame* del volto di un soggetto catturato dalle telecamere, passa in rassegna le immagini custodite nel *database* (la c.d. *watchlist*) per cercare un *match* e, al termine dell'operazione, restituisce un elenco di profili in ordine di probabilità di somiglianza rispetto al soggetto in questione, mandando un segnale di *alert* ove venga trovata una corrispondenza tra volto ignoto e volto schedato[145]. Il sistema, poi, si autoalimenta conservando nel proprio *database* l'immagine del soggetto ignoto anche ove non venga trovato un *match*[146] e registrando i flussi video dalle telecamere. Il *software* è stato progettato anche come soluzione "mobile" per essere installato nel sito ove sorge l'esigenza di disporre dello stesso[147].

Tale sistema, se da un lato è in grado di migliorare il controllo del territorio, dall'altro è potenzialmente pericoloso e solleva diverse perplessità circa possibili violazioni dei diritti costituzionali derivanti da un eventuale utilizzo su larga scala, in particolare considerando che i *database* da cui ad oggi attinge contengono una grandissima mole di dati personali (circa 16 milioni di per-

---

[143] Consultabile al *link*, *https://www.poliziadistato.it/statics/06/20160627-ct-sari--4-.pdf, https://www.poliziadistato.it/statics/17/lotto-2---sari-sistema-di-acquisizione-e-trasmissione-v23---finale--2-.pdf.*

[144] R.V.O. VALLI, *Sull'utilizzabilità processuale del SARI: il confronto automatizzato di volti rappresentati da immagini*, in *Il Penalista*, 16 gennaio 2019.

[145] E. SACCHETTO, *Face to Face: il complesso rapporto tra automated faciale recognition technology e processo penale,* cit., 2020, 9.

[146] LOPEZ, *La rappresentazione facciale tramite software*, cit., 244.

[147] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, 25 marzo 2021 (9575877).

sone, o più)[148]. Oltre alle ovvie criticità in punto di violazione del diritto alla *privacy* dei soggetti ripresi[149], il SARI solleva importanti perplessità con riferimento ai potenziali effetti discriminatori nei confronti dei migranti, dovuti alla mancanza di sistemi adeguati di controllo e verifica volti ad escludere dalla *watchlist* i soggetti richiedenti asilo, a rilevare eventuali *bias* e a garantire trasparenza e accuratezza dell'algoritmo.

Le dinamiche sin qui descritte non possono essere lette come il risultato di una mera sovrapposizione contingente tra tecnologie emergenti e politiche migratorie, né come l'effetto occasionale dell'innovazione tecnica applicata a un ambito tradizionalmente segnato da istanze securitarie. Al contrario, esse rivelano una più profonda convergenza strutturale tra la razionalità propria della *crimmigration* e la logica probabilistica che caratterizza i sistemi di intelligenza artificiale. Entrambe, infatti, si fondano su una grammatica del rischio che legittima l'anticipazione dell'intervento autoritativo, la classificazione preventiva dei soggetti e la compressione delle garanzie individuali in nome della sicurezza pubblica. In tale prospettiva, l'intelligenza artificiale non si limita ad amplificare pratiche già esistenti, ma fornisce alla *crimmigration* un apparato tecnico in grado di tradurre in decisioni automatizzate e apparentemente neutrali presupposti valutativi intrinsecamente selettivi, rafforzando e normalizzando un approccio fondato sulla presunzione di pericolosità del migrante. È proprio questa relazione di reciproco rafforzamento – più che il semplice intersecarsi di due fenomeni distinti – a spiegare la particolare pervasività e criticità dell'impiego dell'IA nel controllo delle frontiere e nella gestione amministrativa e penale dell'immigrazione. Questa relazione di reciproco rafforzamento contribuisce, inoltre, a spostare l'asse della valutazione giuridica dal fatto alla persona[150], dalla condotta alla probabilità, inscrivendo il trattamento dello straniero in una logica attuariale che tende a rendere strutturale l'eccezione e permanente l'emergenza. Il migrante viene così configurato come soggetto paradigmatico della decisione preventiva, destinatario di misure che, pur collocandosi formalmente al di fuori del circuito penale, ne riprodu-

[148] LOPEZ, *La rappresentazione facciale tramite software*, cit., 246.
[149] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, cit.
[150] SCERBO, *Algoritmi predittivi, law enforcement,* in *Arch. pen. web,* 12 dicembre 2025, 7.

cono le logiche, le finalità e i meccanismi repressivi, sottraendosi però alle relative garanzie costituzionali e procedurali[151]. È in questo slittamento, reso possibile dall'innesto della razionalità algoritmica su un terreno già predisposto dalla *crimmigration*, che si coglie il rischio più profondo di una progressiva naturalizzazione della discriminazione, mediata dalla tecnica e legittimata dall'apparente oggettività del calcolo. Attraverso la sorveglianza, la classificazione e il confinamento, i nuovi sistemi intelligenti si configurano, quindi, come strumenti di controllo selettivo su determinate categorie sociali[152], contribuendo ad alimentare e consolidare la progressiva intersezione tra politiche di contrasto alla criminalità e gestione dell'immigrazione.

5. Lotta alla discriminazione e regolamentazione della tecnologia: l'AI Act. Se in campo tecnologico i correttivi alle criticità sin qui delineate stanno arrivando dalla scienza informatica, grazie alla creazione di meccanismi *anti-bias* che consentano di selezionare la tipologia di dati da aggiungere a quelli già presenti nell'algoritmo per correggerne le distorsioni, oppure di ricampionare le immagini in funzione del colore della pelle del soggetto da riconoscere[153], le risposte giuridiche arrivano prima di tutto dalle fonti internazionali, ed in particolare da strumenti di *soft law*.

Nel corso del tempo, infatti, sono stati elaborate diversi testi volti a disciplinare l'impiego delle tecnologie digitali e, più recentemente, dell'intelligenza artificiale, con particolare attenzione alla tutela dei diritti fondamentali – che costituiscono il «perimetro entro cui discutere della legittimazione normativa di qualsiasi innovazione tecnico-scientifica»[154] – e alla prevenzione di pratiche discriminatorie.

Va menzionata, innanzitutto, la Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, emanata il 4 dicembre 2018 in seno al Consiglio d'Europa ed elaborata dalla CEPEJ. La Carta elabora cinque principi per favorire un utilizzo consapevole delle nuove tecnolo-

---

[151] *Ibid.*, 97.

[152] MILLER, *Blurring the Boundaries Between Immigration and Crime Control after Sept. 11th*, cit., 98.

[153] LOPEZ, *La rappresentazione facciale tramite software*, cit., 247.

[154] CIANITTO, *Libertà religiosa e AI*, in *Intelligenza Artificiale, Diritto, giustizia, economia ed etica*, a cura di Basile-Biasi-Camaldo-Caneschi, Fragasso-Milani, cit., 255.

gie nel sistema della giustizia, tra cui spicca quello di non discriminazione, volto a «prevenire lo sviluppo o l'intensificazione di qualsiasi discriminazione tra persone o gruppi di persone»[155]. La Carta chiede agli attori pubblici e privati di assicurare che le metodologie dell'IA non riproducano o aggravino le discriminazioni e non conducano ad analisi o usi deterministici, predisponendo una particolare vigilanza tanto nella fase di elaborazione dei *software* che in quella di utilizzo degli stessi, in particolar modo ove vengano trattati dati sensibili[156].

Rilevanti, poi, sempre con riferimento al principio di non discriminazione, sono: la Risoluzione del Parlamento europeo n. 2015/2103(INL) del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica; la Risoluzione del Parlamento europeo n. 2018/2088(INI) del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale; gli Orientamenti etici per un'intelligenza artificiale affidabile adottati dal gruppo di esperti istituito dalla Commissione europea nell'aprile 2019; il Libro bianco sull'intelligenza artificial nella PA adottato dall'Agenzia per l'Italia digitale nel marzo 2018. Tutti testi, questi, che valorizzano la necessità di un approccio cauto all'intelligenza artificiale il cui impiego, seppur incentivato, necessita di adeguati correttivi.

È opportuno citare, poi, a livello internazionale, il rapporto pubblicato nel 2020 dall'Assemblea generale delle nazioni unite intitolato «*Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis*» che ha reso evidente al mondo intero i rischi posti dall'avanzamento tecnologico, imponendo agli Stati l'obbligo di contrastare e prevenire ogni utilizzo delle tecnologie che possa causare discriminazioni, anche nel caso in cui tali sistemi siano sviluppati e impiegati da soggetti privati piuttosto che da autorità statali.

Per quanto concerne gli strumenti di *hard law*, va senza dubbio menzionata la Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 (nota come *Law Enforcement Directive*), relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità statali nell'esercizio di funzioni di prevenzione dei reati, indagine e

[155] CEPEJ, *Carta etica per l'uso dell'intelligenza artificiale*, cit., 8.
[156] *Ibid.,* 8.

accertamento penale, recepita in Italia con il citato d.lgs. 51/2018. Di particolare rilievo è l'articolo 11, che impone agli Stati membri di vietare le decisioni basate esclusivamente su trattamenti automatizzati di dati, inclusa la profilazione, che abbiano effetti giuridici negativi o incidano significativamente sugli interessati. La disposizione, inoltre, vieta che tali decisioni possano fondarsi su dati sensibili, come quelli relativi all'origine razziale, alle opinioni politiche o alle convinzioni religiose, a meno che non siano previste adeguate garanzie a tutela dei diritti delle persone, tanto a livello nazionale quanto europeo.

Nonostante l'elevata quantità di raccomandazioni, risoluzioni, carte etiche e orientamenti, l'Unione europea ha sofferto, fino al 2023, della mancanza di una disciplina di *hard law* che regolamentasse in modo completo ed esaustivo la materia dell'intelligenza artificiale, consentendone un utilizzo più sicuro e rispettoso dei diritti fondamentali.

Per tale ragione, nel 2021 la Commissione europea ha pubblicato una proposta di direttiva del Parlamento europeo e del Consiglio sull'intelligenza artificiale, un *corpus* normativo articolato che mirava a disciplinare la materia in maniera organica, adottando un approccio normativo orizzontale. L'obiettivo dichiarato era quello di stabilire principi e requisiti minimi essenziali per la regolamentazione dei sistemi di intelligenza artificiale, soprattutto in ambiti di particolare delicatezza. Nel marzo 2024 è stato promulgato il Regolamento definitivo[157], composto da 113 articoli (e tredici allegati) di cui il primo afferma che: «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo al contempo un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione Europea, inclusi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, nonché promuovere l'innovazione».

I destinatari del regolamento sono sia soggetti pubblici che privati, operanti all'interno e all'esterno dell'Unione europea, a condizione che il sistema di

[157] Definito come l'emblema di una «nuova fase del costituzionalismo digitale» (POLLICINO, *Costituzionalismo digitale. Pensare la democrazia al tempo dell'IA*, Bologna, 2025, 181).

IA sia immesso sul mercato dell'Unione stessa o che il suo utilizzo abbia effetti su persone situate all'interno di essa.
Il testo propone un interessante approccio basato su una classificazione dei rischi, suddivisi in quattro categorie: a) rischio inaccettabile, riguardante una serie limitata di utilizzi dell'intelligenza artificiale in contrasto con i valori dell'UE e i diritti fondamentali, che saranno pertanto sempre vietati; b) rischio alto, che interessa un numero ristretto di sistemi che potrebbero avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali, relativamente ai quali non vi è un divieto, ma è prevista una regolamentazione rigorosa; c) rischio minimo, concernente sistemi che possono essere utilizzati in conformità con la legislazione vigente, senza ulteriori obblighi; d) rischio sistemico, che riguarda modelli generali di IA.
Prima di classificare le pratiche all'interno delle diverse categorie di rischio, il Regolamento prevede alcune esclusioni, su cui torneremo più avanti e che costituiscono, a parer nostro, un grave *vulnus* per le tutele apprestate.
Tornando ai livelli di rischio, il capo II è dedicato alle «pratiche di intelligenza artificiale vietate», relative, chiaramente, a soglie di rischio inaccettabile, che vengono individuate dall'art 5. L'articolo si riferisce ad un numero totale di otto pratiche, a fronte delle quattro originariamente proposte dalla Commissione nell'aprile 2021[158], tra cui rientrano, ad esempio, i sistemi che impiegano tecniche manipolative (art. 5, lett. a) o i sistemi che consentono ad attori pubblici o privati di attribuire un punteggio sociale alle persone fisiche (art. 5 lett. c).
Per quanto di nostro interesse, tuttavia, preme evidenziare l'inserimento, tra le pratiche vietate, dei seguenti gruppi di sistemi: alla lett. d), sistemi di valutazione del rischio di commissione di reati basati esclusivamente sulla profilazione dei tratti della personalità, rispetto ai quali il Regolamento sottolinea che, conformemente al principio della presunzione di innocenza, le persone fisiche all'interno dell'Unione devono essere giudicate solo sulla base del proprio comportamento concreto e non su previsioni elaborate da sistemi di IA basati esclusivamente sulla profilazione o su tratti personali, quali cittadi-

[158] LEVANTINO-NERONI REZENDE, *Rischio inaccettabile: usi proibiti*, in *La disciplina dell'intelligenza artificiale,* a cura di Finocchiaro-Palmirani-Pollicino-Vaciago-Ziccardi, cit., 159.

nanza, luogo di nascita, residenza, numero di figli, livello di indebitamento o tipo di automobile posseduta, in assenza di ragionevoli sospetti fondati su fatti oggettivi verificabili; alla lett. e), sistemi che amplino le banche dati di riconoscimento facciale mediante il prelievo di foto e immagini da internet o da filmati di telecamere a circuito chiuso; alla lett. g), sistemi di categorizzazione biometrica che classifichino le persone sulla base delle loro caratteristiche biometriche al fine di trarne deduzioni in merito alla razza, alle opinioni politiche o sindacali, religiosi, o all'orientamento sessuale; alla lett. h), sistemi di identificazione biometrica a distanza in tempo reale in spazi pubblicamente accessibili (in questo caso l'uso è consentito ove sia strettamente necessario per: la ricerca di vittime di reato, comprese le persone scomparse; la prevenzione di minacce specifiche alla vita o all'incolumità fisica delle persone; la prevenzione di attacchi terroristici; la localizzazione e identificazione di autori o sospetti di reati elencati nell'allegato del regolamento, che prevedano pene privative della libertà personale di almeno quattro anni ed anche in tali casi, comunque, il sistema dovrà essere utilizzato al solo fine di identificare la persona interessata e tenere conto della gravità della situazione e dell'eventuale danno causato dal proprio uso, in particolare per quanto riguarda le conseguenze per i diritti e le libertà dei soggetti coinvolti, solo successivamente ad una valutazione, da parte dell'autorità di contrasto, dell'impatto sui diritti fondamentali che l'uso del sistema avrà e previa registrazione del sistema nella banca dati UE appositamente creata). Il Regolamento specifica poi che nessuna decisione pregiudizievole può essere adottata esclusivamente sulla base dei risultati generati dal sistema di identificazione biometrica, trattandosi di strumenti particolarmente invasivi per quanto concerne i diritti e le libertà delle persone interessate, che incidono negativamente sulla vita privata di ampi segmenti della popolazione, generando una percezione costante di sorveglianza, scoraggiando così indirettamente l'esercizio della libertà di riunione e di altri diritti fondamentali, oltre ad essere caratterizzati da inesattezze di carattere tecnico che possono determinare risultati distorti e comportare effetti discriminatori.

Il capo III è dedicato ai sistemi ad alto rischio, elencati dall'articolo 6, il quale specifica che un sistema di intelligenza artificiale è considerato ad alto rischio

se soddisfa, cumulativamente, due condizioni: è destinato ad essere impiegato come componente di sicurezza di un prodotto o è esso stesso un prodotto, e tale prodotto è soggetto a valutazione di conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio nell'UE. Oltre a tali sistemi, il paragrafo due rimanda ad un elenco contenuto nell'allegato III al Regolamento, tra cui, per quanto di nostro interesse, vengono compresi, oltre ai sistemi di identificazione biometrica remota o di categorizzazione biometrica sulla base di attributi o caratteristiche sensibili, i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti in materia di migrazione, asilo e gestione del controllo delle frontiere.

Nello specifico, vengono classificati come ad alto rischio: i poligrafi (e strumenti analoghi); gli strumenti impiegati per valutare un rischio (per la sicurezza statale, di immigrazione irregolare o per la salute nazionale) posto da una persona che intenda entrare nei confini dello Stato membro; i sistemi destinati ad assistere le autorità nell'esame delle domande di asilo, visto o permesso di soggiorno sia per quanto riguarda l'ammissibilità delle persone che per la valutazione sull'affidabilità degli elementi probatori; i sistemi destinati all'individuazione, al riconoscimento e all'identificazione di persone fisiche. Il Regolamento ritiene opportuno classificare come ad alto rischio queste pratiche in ragione del fatto che tali strumenti hanno effetti su persone che si trovano spesso in una posizione particolarmente vulnerabile e il cui futuro dipende dall'esito delle azioni delle autorità pubbliche competenti. L'accuratezza, la natura non discriminatoria e la trasparenza dei sistemi di IA utilizzati in tali contesti sono pertanto particolarmente importanti per garantire il rispetto dei diritti fondamentali delle persone interessate, in particolare i loro diritti alla libera circolazione, alla non discriminazione, alla protezione della vita privata e dei dati personali, alla protezione internazionale e alla buona amministrazione.

I sistemi di cui all'allegato III, comunque, non sono considerati ad alto rischio se non presentano rischi significativi di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, o comunque quando non influenzino materialmente il risultato del processo decisionale perché destinati ad eseguire compiti procedurali limitati, a migliorare risultati già raggiunti da

una precedente attività umana, a rilevare schemi decisionali o deviazioni da schemi precedenti senza sostituire o influenzare la valutazione umana già completata, ovvero a svolgere un compito meramente preparatorio[159].

Tale ultima disposizione desta preoccupazione poiché costituisce una definizione estremamente vaga ed indeterminata che porta, in definitiva, ad annullare le garanzie poste per i sistemi ad alto rischio. La necessità di intervento umano, seppur prevista, rischia di diventare sterile in alcuni ambiti in cui la decisione umana si appiattisce, in modo del tutto acritico e formale, al risultato fornito dalla macchina[160]. Occorre, infatti, tenere sempre presente il rischio di "cattura" della decisione da parte del sistema tecnologico (fenomeno di *anchoring*), con l'ulteriore difficoltà, nella pratica, di provare effettivamente quando ciò sia avvenuto e quando invece essa sia stata autonoma[161]. Sarà necessario, sul punto, adottare un'interpretazione sostanziale del regime di non esclusività della decisione automatizzata, riconducendo a tale concetto anche i casi in cui l'intervento umano esista ma sia meramente formale e privo di qualsivoglia valutazione attiva[162].

Il Regolamento prevede, poi, la possibilità per la Commissione di ampliare l'elenco di cui all'Allegato III nel caso di sistemi operanti negli ambiti indicati dallo stesso allegato, che presentino un rischio per la salute, la sicurezza o i diritti fondamentali equivalente o superiore a quello presentato dai sistemi ivi già inclusi. Tale valutazione dovrà tener conto di fattori quali la quantità di dati utilizzati e trattati, le finalità del sistema, il livello di autonomia e di controllo umano, la potenziale capacità di causare danni gravi o di incidere negativamente su specifiche persone o gruppi, nonché la correggibilità dei risultati prodotti dal sistema.

L'utilizzo dei sistemi classificati ad alto rischio e delle relative pratiche è quindi consentito ma subordinato a una serie di requisiti stringenti, disciplinati ne-

---

[159] Essi sono quindi considerati "ad alto rischio" sulla scorta di una presunzione *iuris tantum* facilmente superabile (così PULITO, *Algoritmi predittivi e valutazione della pericolosità sociale: livelli di rischio alla luce dell'AI Act e prospettive interne di impiego*, in *Arch. pen. web*, 21 novembre 2025, 13).

[160] DELLA TORRE, *Novità del Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, cit., 235.

[161] ZUDDAS, *Intelligenza artificiale e discriminazioni*, cit., 474.

[162] MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 198.

gli artt. 8 e seguenti del Regolamento: a) l'istituzione ed attuazione di un sistema di gestione dei rischi, inteso come «percorso iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio»[163] che identifichi *ex ante* i rischi e adotti misure mirate intese ad affrontarli; b) la soggezione dei *set* di dati di addestramento a pratiche di *governance* che riguardino i processi di raccolta, il trattamento, l'esame di possibili distorsioni discriminatorie e l'attuazione di misure adeguate ad evitarle; c) la sufficiente rappresentatività dei *set* di dati, che dovranno tener conto dello specifico ambito geografico di utilizzo; d) la trasparenza del funzionamento dell'algoritmo, tale da consentire ai *deployer* di interpretare correttamente l'*output*, anche attraverso la fornitura di istruzioni per l'uso in formato digitale che contengano una serie di elementi indicati dall'art. 13; e) l'obbligo di sorveglianza umana in modo commisurato ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA. Il regolamento specifica anche che gli utilizzatori dovranno essere sempre consapevoli della tendenza a fare automaticamente affidamento sull'*output* prodotto dal sistema e della possibilità di ignorare tale *output*. Inoltre, specificamente per i sistemi di identificazione biometrica, è previsto l'obbligo di verifica e conferma separata da parte di almeno due persone prima che il *deployer* compia azioni o adotti decisioni basate sui risultati forniti dal sistema; f) la predisposizione, da parte dei fornitori, di sistemi di gestione della qualità e della conformità al Regolamento e di misure volte a correggere o disabilitare il sistema nel caso in cui esso sia messo in servizio non in conformità con il Regolamento stesso; g) l'obbligo di informazione e cooperazione con le autorità competenti, sia per i fornitori che per gli utilizzatori; h) l'obbligo di valutare l'impatto sui diritti fondamentali, identificando, per ogni sistema che viene creato o immesso sul mercato, i processi in cui il sistema sarà utilizzato, il periodo di tempo in cui sarà utilizzato, le categorie di soggetti verosimilmente interessate dal suo uso, i rischi di danno, le misure di sorveglianza umana adottate e le misure correttive eventualmente attivabili.

Il rispetto delle regole previste sarà garantito mediante la predisposizione di una serie di controlli e l'istituzione presso ogni Stato membro di autorità ed

[163] Art. 9, co. 2 lett. a) AI Act.

organismi indipendenti di vigilanza, oltre che dalla creazione di un Ufficio Europeo per l'IA, con lo specifico compito di applicare e supervisionare il rispetto della nuova disciplina. Gli Stati membri, poi, dovranno garantire l'applicazione di sanzioni effettive, proporzionate e dissuasive in caso di violazione del Regolamento.

6. *La nuova disciplina italiana: la L. 23 settembre 2025 n. 132.* Con la L. 23 settembre 2025, n. 132 il Parlamento ha emanato "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", predisponendo per la prima volta nel nostro Paese, un impianto normativo esaustivo sul tema.
Il testo si pone in continuità con la normativa europea, dalla quale, infatti, prende in prestito anche le definizioni iniziali di «sistema di intelligenza artificiale» e «modelli di intelligenza artificiale»[164]. Come quello sovranazionale, il legislatore italiano sceglie un approccio "aperto" all'intelligenza artificiale e ai suoi benefici per lo sviluppo economico-sociale, adottando una posizione di equilibrio fra l'obiettivo dichiarato di promuovere un utilizzo dell'IA trasparente, corretto, e responsabile e quello di garantire, pur sempre, una stretta vigilanza sui rischi che da essa derivino per i diritti fondamentali dei soggetti coinvolti.
La legge si articola in sei capi, di cui il primo è dedicato – oltre che alle definizioni – a stabilire i principi rilevanti in materia, tra i quali campeggia il rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione e dal diritto dell'Unione europea. Il capo II è dedicato alla disciplina dell'utilizzo e dello sviluppo di sistemi di intelligenza artificiale in alcuni ambiti: sanitario, lavorativo, nella pubblica amministrazione, nell'attività giudiziaria. Il capo III è dedicato a strategia nazionale, autorità nazionali e azioni di promozione e contiene disposizioni dedicate alla creazione e al coordinamento di Autorità indipendenti in materia di IA, alle strategie di collaborazione tra enti, amministrazioni pubbliche e soggetti coinvolti a vario titolo nelle fasi di *governance*, nonché una serie di deleghe al Governo (art. 24). Il capo IV è dedicato alla tutela del diritto d'autore delle opere generate con l'IA, mentre il capo V è dedicato alle disposizioni penali e il Capo VI contiene le disposizioni finali e

[164] Art. 2, L.. 23 settembre 2025, n. 132.

finanziarie[165].

Per quanto qui di interesse, assume rilievo, in primo luogo, l'art. 6, il quale prevede l'esclusione dall'ambito di applicazione della disciplina nazionale delle attività di ricerca, sperimentazione, sviluppo, adozione e utilizzo di sistemi di intelligenza artificiale qualora esse siano svolte per finalità di sicurezza nazionale, nozione definita in senso ampio mediante rinvio a una pluralità di fonti normative in materia di *intelligence*, cybersicurezza, difesa nazionale e contrasto alla criminalità grave. Il legislatore precisa che tale esclusione non può in ogni caso pregiudicare il rispetto dei diritti fondamentali e delle libertà costituzionali, lo svolgimento democratico della vita istituzionale e politica, nonché i principi di autonomia e sussidiarietà, il dibattito democratico e la sovranità dello Stato.

Rileva, inoltre, l'art. 24, che, nel conferire deleghe al Governo in materia di intelligenza artificiale, prevede, al co. 2, lett. h), l'adozione di una disciplina specifica per l'utilizzo di sistemi di IA nell'ambito dell'attività di polizia. Infine, merita menzione l'art. 26, che introduce una serie di modifiche al codice penale, includendo, accanto a una delega per l'introduzione di nuove fattispecie di reato, una specifica ipotesi di illecita diffusione di contenuti generati o manipolati artificialmente, una nuova figura di reato in materia di violazione del diritto d'autore, nonché una circostanza aggravante comune e alcune aggravanti speciali.

Muovendo dall'analisi dell'art. 6, possono richiamarsi le criticità già evidenziate con riferimento alle esclusioni previste dall'AI Act europeo, le quali, nel recepimento nazionale, risultano ulteriormente accentuate. A differenza della normativa europea, infatti, la L. n. 132 del 2025 omette qualsiasi riferimento all'utilizzo dei sistemi di intelligenza artificiale nel controllo delle frontiere e nella gestione dei flussi migratori, non predisponendo sin dall'origine alcuno spazio di tutela specificamente rivolto ai soggetti migranti. Se il legislatore europeo è già stato oggetto di rilievi critici per aver delineato possibili vuoti di protezione nell'area della sicurezza nazionale, il legislatore interno sembra spingersi oltre, escludendo in radice tale ambito dall'orizzonte di regolazione,

[165] Per un'attenta analisi dei profili penalistici del *corpus* normativo v. FRAGASSO, *Profili penalistici della legge sull'intelligenza artificiale: osservazioni a prima lettura*, in *Sist. pen.*, 2025, 10, 157 ss.

con il rischio di legittimare pratiche potenzialmente lesive dei diritti fondamentali.
In tale contesto, la clausola di salvaguardia contenuta nell'art. 6, che richiama il doveroso rispetto dei diritti fondamentali, appare insufficiente a prevenire le distorsioni discriminatorie emerse nei precedenti capitoli, specie ove si consideri l'eventuale impiego non regolamentato di sistemi di intelligenza artificiale nella valutazione della pericolosità del migrante. Il rischio si accentua se tale esclusione viene letta congiuntamente alla delega conferita al Governo dall'art. 24, co. 2, lett. h), per l'adozione di una disciplina sull'utilizzo dell'IA nell'attività "di polizia", espressione ampia e priva di ulteriori specificazioni. Ne deriva il timore che, in un futuro non lontano, possano essere introdotte disposizioni che, da un lato, legittimino l'impiego di strumenti algoritmici durante le attività di controllo delle frontiere o di gestione dei rimpatri (passibili, forse, di rientrare nella categoria delle "attività di polizia") e, dall'altro, ne sottraggano l'utilizzo alle garanzie previste dalla legge in commento, in virtù dell'eccezione per la sicurezza nazionale di cui all'art. 6.

7. *Conclusioni.* Analizzate le principali innovazioni introdotte dall'AI Act e dalla L. 132/2025, appare ora opportuno fornire una risposta all'interrogativo di fondo sollevato in sede introduttiva: se, cioè, il nuovo impianto normativo consenta di configurare un impiego dell'intelligenza artificiale che risulti pienamente conforme e rispettoso dei diritti fondamentali degli individui coinvolti.
Con riguardo alla normativa europea sembra potersi affermare, in definitiva, che il Regolamento rappresenti una svolta paradigmatica nell'approccio regolatorio dell'Unione in materia. A differenza delle precedenti iniziative normative – spesso incentrate prevalentemente sui rischi per la sicurezza derivanti dall'utilizzo delle tecnologie algoritmiche – il nuovo regolamento manifesta una decisa attenzione per le implicazioni etico-giuridiche e per la tutela dei diritti fondamentali. Particolarmente rilevanti, sul punto, risultano le disposizioni relative all'obbligo di trasparenza dei processi decisionali algoritmici, alla necessità di una preventiva valutazione d'impatto sui diritti fondamentali e all'imposizione di *standard* qualitativi rigorosi concernenti la rappresentatività,

l'accuratezza e l'assenza di *bias* nei dati utilizzati. Tali prescrizioni, infatti, rappresentano pilastri normativi essenziali per prevenire le disfunzioni e le distorsioni illustrate nei paragrafi 1 e 2. In virtù di queste garanzie, e del complesso dei divieti e limitazioni che concorrono a rafforzarne l'efficacia applicativa, si può pertanto ritenere che l'AI Act consenta di delineare un utilizzo dell'intelligenza artificiale, perlomeno in alcuni settori, che sia compatibile con le esigenze di protezione dei diritti inviolabili della persona.

Nel settore della giustizia penale, ad esempio, la scelta del legislatore europeo, pur adottando una posizione di tutela "forte" dei diritti fondamentali nel vietare decisioni basate su caratteristiche personali, lascia comunque aperto il campo a possibili utilizzi dei sistemi predittivi in senso positivo per il destinatario. Al di fuori, quindi, dei casi di sostituzione completa dell'algoritmo con il giudice, non vi è un divieto di impiego dell'intelligenza artificiale, ma vengono forniti degli *standard* a cui adeguarsi per far sì che l'intervento automatizzato sia rispettoso dei diritti inviolabili e costituzionalmente orientato[166]. Sul punto, si pensi a sistemi che, basando le proprie predizioni su comportamenti e non su caratteristiche personali, permettano di valutare la c.d. buona condotta (o meglio, l'adesione al percorso trattamentale) dei detenuti, al fine di coadiuvare la magistratura di sorveglianza nell'adozione di decisioni sulla libertà anticipata o sulla concessione di misure alternative per combattere il fenomeno del sovraffollamento (come avvenuto in America grazie al *software* PATTERN) oppure, ancora, a sistemi che supportino il giudice nella nuova fase di *sentencing* prevista dall'art. 545*bis* c.p.p., valutando la pena sostitutiva più adatta per un determinato individuo sulla base dei documenti acquisiti e delle interlocuzioni con l'Ufficio di Esecuzione penale esterna e con il condannato stesso. In tal modo, sfruttando il potenziale informativo che l'algoritmo può fornire al giudice[167], si perseguirebbe una maggiore individualizzazione della pena, progettuale e adeguata alla reale potenzialità di rieduca-

[166] GULOTTA-EGNOLETTI-NICCOLAI-PAGANI, *Tendenze generali e personali ai bias cognitivi e la loro ricaduta in campo forense: fondamenti e rimedi,* in *www.sistemapenale.it,* 11 giugno 2021, 5.

[167] MALDONATO, *Algoritmi predittivi del rischio di recidiva: questioni problematiche e nuove prospettive*, in *Forme, riforme e valori per la giustizia penale futura*, Napoli, a cura di Castronuovo-Negri, 2023, 206 ss.

zione del condannato[168], sempre favorendo un'interpretazione dell'art. 133, co. 2 c.p. in armonia con i principi fissati dagli artt. 3 e 27 della Costituzione. In quest'ottica, il decisore non verrebbe privato del suo autonomo potere valutativo e lo strumento tecnologico ricoprirebbe per esso una funzione collaborativa ed ancillare[169], senza però basare il proprio *output* su caratteristiche personali del soggetto da cui potrebbero derivare distorsioni discriminatorie. Ovviamente, l'incontro tra modernizzazione e rispetto dei diritti del condannato dovrà sempre essere garantito da un controllo motivazionale critico, che mostri di aver prestato la dovuta attenzione individualizzante al caso specifico, oltre che una piena conoscenza del funzionamento dell'algoritmo e dei relativi rischi[170].

Per quanto concerne l'impiego di sistemi di intelligenza artificiale nel contesto del controllo delle frontiere, tuttavia, pare necessario giungere a conclusioni parzialmente diverse. In tale ambito, infatti, l'AI Act sembra non aver soddisfatto a pieno le aspettative in quanto, accanto all'introduzione delle tutele, si affianca una tendenza al parziale annullamento delle garanzie predisposte, mediante il continuo riferimento alla possibilità di "eccezioni" all'applicabilità del Regolamento stesso. L'art. 2, co. 2, prevede infatti che il compendio normativo non pregiudichi le competenze degli Stati membri in materia di sicurezza nazionale, escludendo dal proprio ambito di applicazione tutti i sistemi di IA immessi sul mercato, messi in servizio o utilizzati per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività, e dei sistemi e i modelli di IA specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici.

Se tali eccezioni non sembrano comportare un rischio elevato per i sistemi

---

[168] Sulla necessaria progettualità della pena e la relativa importanza del nuovo art. 545*bis* c.p.p., v. *amplius* EUSEBI, *La pena tra necessità di strategie preventive e nuovi modelli di risposta al reato*, in *Riv. it. dir. proc. pen.*, 2021, 3, 823 ss.; EUSEBI, *Pene retributive e giustizia riparativa*, in *Forme, riforme e valori per la giustizia penale futura*, a cura di Castronuovo-Negri, Napoli, 2023, 365 ss.; EUSEBI, *Giustizia riparativa e riforma del sistema sanzionatorio penale*, in *Dir. pen. proc.,* 2023, 1, 79 ss, EUSEBI, *Giustizia punitiva e giustizia riparativa: quali rapporti?,* in *disCrimen*, 3 ottobre 2023., EUSEBI, *Il cantiere lento della riforma in materia di sanzioni penali. Temi per una discussione*, in *Arch. pen.*, 2022, 1, 1.

[169] FIORELLI-GONNELLA-MASSARO-RICCARDI-RUOTOLO-TALINI, *Pena e nuove tecnologie: tra trattamento e sicurezza,* Napoli, 2022.

[170] GULOTTA-EGNOLETTI-NICCOLAI-PAGANI, *Tendenze generali e personali ai bias cognitivi e la loro ricaduta in campo forense: fondamenti e rimedi,* cit., 9.

impiegati in ambito giurisdizionale, ove difficilmente potrebbero essere invocate, i problemi nascono quando i *software* vengono utilizzati nella gestione dei flussi migratori. La presenza della clausola che prevede l'esclusione dell'applicabilità dei divieti in situazioni in cui sia in gioco la sicurezza nazionale mina, di fatto, in modo velato, le garanzie offerte dall'AI Act nei confronti dei migranti, i quali, frequentemente, si trovano a essere soggetti all'uso di tecnologie intelligenti giustificato proprio sotto l'egida della sicurezza nazionale. Si ricordi, infatti, che è proprio in nome della pubblica sicurezza e dell'ordine pubblico, e del presunto pericolo che un soggetto potrebbe rappresentare per essi, che i richiedenti asilo e i migranti possono essere respinti alle frontiere degli Stati membri. Questa ampia deroga, ripresa anche dalla normativa nazionale, solleva rilevanti preoccupazioni, in quanto esclude da un regime di vigilanza rafforzata proprio quegli ambiti in cui le tecnologie di IA risultano potenzialmente più invasive, rafforzando una preoccupante asimmetria nella protezione dei diritti laddove i soggetti coinvolti siano stranieri, apolidi ed immigrati in generale. Anche per quanto riguarda le tecnologie di identificazione biometrica a distanza in tempo reale, le numerose eccezioni all'applicabilità del divieto, sempre collegate alla necessità di perseguire gravi forme di reato[171], annullano, di fatto, l'efficacia del divieto stesso nei confronti degli immigrati i cui dati siano contenuti nella banca dati AFIS. In alcuni casi, poi, l'AI Act pare addirittura fornire una base legale, prima invero inesistente, ad alcune pratiche particolarmente pericolose (si pensi alle tecnologie di riconoscimento delle emozioni, prive di regolamentazione fino all'introduzione del testo)[172].

Un correttivo potrebbe consistere nell'inserire l'utilizzo *di risk assesment tools* in ambito di controllo delle frontiere tra le pratiche vietate di cui all'art. 5, co. 1, lett. d), accanto a quelle utilizzate per prevedere la possibilità di futura commissione dei reati; mentre l'utilizzo di sistemi di sorveglianza volti a prevedere le rotte migratorie al fine di evitare l'arrivo al confine delle popolazioni in movimento dovrebbe figurare tra le pratiche vietate *ex* art. 5, co. 1,

[171] CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, in *Intelligenza Artificiale, Diritto, giustizia, economia ed etica*, a cura di Basile-Biasi-Camaldo-Caneschi, Fragasso-Milani, cit., 77.

[172] AMNESTY INTERNATIONAL, *Open Letter to the Rapporteurs on the Eu Artificial Intelligence Regulation (AI Act) to Ensure Protection of Rights of Migrants, Asylum Seekers and Refugees*, 26 aprile 2023.

lett. h), sì da controbilanciare il divieto con le eccezioni ivi previste, soprattutto in tema di tratta di esseri umani. Anche in materia di espulsione, respingimento e detenzione amministrativa pre-rimpatrio, sarebbe auspicabile una specifica legislazione interna volta a limitare l'utilizzo di sistemi tecnologici a supporto delle relative decisioni, quantomeno se volte a calcolare la "pericolosità" dello straniero sulla base di caratteristiche personali.

In ogni caso, la promessa di velocizzazione e semplificazione delle procedure decisorie, se da un lato rappresenta una chimera per gli addetti ai lavori, non può e non deve oscurare la pressante esigenza di aumentare le garanzie e i diritti dei migranti, favorendo una loro integrazione e combattendone la graduale criminalizzazione.

Pur riconoscendo, quindi, il valore innovativo e l'apprezzabile impulso garantistico della normativa esaminata, non può omettersi una riflessione critica con riferimento al settore particolarmente sensibile della gestione dei flussi migratori, ambito in cui il quadro si presenta ancora parziale e bisognoso di un'integrazione sistemica, volta a cogliere in maniera più puntuale le specificità del rapporto tra transizione digitale e condizione giuridica del migrante. In attesa, quindi, di ulteriori interventi normativi che affrontino in modo dedicato le implicazioni dell'automazione nella gestione della mobilità umana, il sentiero verso una soluzione che concili modernizzazione e diritti fondamentali sembra snodarsi sul campo della programmazione degli algoritmi e sulla configurazione dei *set* di dati di addestramento, uniti ovviamente ad un impegno educativo volto all'integrazione tra dimensione tecnica e dimensione etica, anticipando la tutela dei valori costituzionali, tra i quali il principio di non discriminazione, già in fase di progettazione dell'algoritmo[173]. Ciò richiederà impegno per l'educazione dei programmatori, al fine di aumentare la consapevolezza degli stessi sui possibili effetti discriminatori degli algoritmi di *machine learning*[174], oltre che dei proprietari delle imprese produttrici e, soprattutto, degli utilizzatori finali, soggetti pubblici o privati che siano, sì da creare

[173] ZUDDAS, *Intelligenza artificiale e discriminazioni*, cit., 470.

[174] Sul punto gli Orientamenti etici per un AI Affidabile suggeriscono di costituire *team* di progettisti provenienti da contesti, culture e discipline diverse, sì da garantire una maggiore rappresentatività in fase di scelta dei *data training sets* (cfr. COMMISSIONE EUROPEA, GRUPPO INDIPENDENTE DI ESPERTI AD ALTO LIVELLO SULL'INTELLIGENZA ARTIFICIALE, *Orientamenti Etici per un'IA affidabile,* 8 aprile 2019).

una sensibilità comune sulle implicazioni etiche delle decisioni algoritmiche[175].
Il progresso, inoltre, dovrà fare i conti con la possibilità che gli algoritmi generino nuove figure soggettive di discriminazione, affiancando alle categorie tradizionalmente svantaggiate, anche "generazioni" di soggetti vittime di discriminazioni indirette ed auto-generatesi da processi di *machine-learning*[176].
Sarà il tempo, dunque, il giudice ultimo della capacità del nostro ordinamento di adattarsi al ritmo incalzante e trasformativo dell'intelligenza artificiale; nella speranza che essa diventi, nel futuro prossimo, non solo motore d'innovazione, ma anche garante di equità, inclusione e rispetto dei diritti fondamentali delle categorie più vulnerabili della società.

[175] ZUDDAS, *Intelligenza artificiale e discriminazioni*, cit., 471.
[176] *Ibid.*, 472.