FEDERICA DE SIMONE

Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale

La libera circolazione di uomini, merci e denaro, simbolo delle democrazie moderne ed espressione di libertà e rispetto dei diritti fondamentali, ha indubbiamente favorito il processo di globalizzazione ma al contempo ha determinato un incremento dei crimini transfrontalieri, tra cui riciclaggio, traffico di armi, di arte e di droga, reati ambientali. Nel tentativo di ampliare gli strumenti di contrasto e garantire la sicurezza dell'area Schengen, l'Unione europea ha finanziato la sperimentazione del progetto "*IBorderCtrl*", un complesso sistema di intelligenza artificiale composto da un rilevatore di inganno e uno strumento di riconoscimento facciale, capaci di coadiuvare le guardie di frontiera nelle attività di verifica delle identità e prevenzione di gravi crimini. Lo sviluppo tecnologico ha sempre portato a significativi cambiamenti per l'umanità e intorno ai sistemi di intelligenza artificiale ci sono grandi aspettative. Grandi, però, sono anche i rischi in termini di tenuta del sistema giuridico, in riferimento al rispetto dei principi e dei diritti fondamentali, soprattutto quando dietro questi strumenti si celano istituti – come le misure di prevenzione – che già sollevano dubbi di legittimità.

A new typology of prevention measures: algorithms, artificial intelligence and facial recognition

The free movement of men, goods and money, a symbol of modern democracies and an expression of freedom and respect for fundamentals rights, has undoubtedly favored the globalization process but at the same time has led to an increase in cross-border crimes, including money laundering, arms, art and drugs trafficking, environmental crimes. In an attempt to broaden law enforcement tools and ensure the security of the Schengen area, the European Union financed the experimentation of the "IBorderCtrl" project, a complex artificial intelligence system consisting of a deception detector and a facial recognition tool, capable of assisting border guards in identity verification and serious crime prevention activities. Technological development has always led to significant changes for people and artificial intelligence systems have created great expectations. Great, however, are also the risks in terms of the stability of the legal system, with reference to respect for principles and fundamental rights, especially when behind these instruments are concealed legal concepts - such as preventive measures - that already raise doubts of legitimacy.

1. *Le nuove modalità di controllo.* «*Nothing to declare? This is your passport, thank you and have a nice trip!* ». Queste, sino a qualche tempo fa, le frasi di

rito al passaggio delle frontiere europee. A esse corrispondeva un timbro sul passaporto, segno formale del superamento dei confini, esibito con orgoglio da ogni viaggiatore che si sentiva cittadino del mondo.

Sono passati poco più di 35 anni dagli Accordi di Schengen, ossia da quando il controllo delle frontiere dei Paesi europei ha assunto una rilevanza sovranazionale, ma forse all'epoca le evidenti esigenze di mobilità delle persone e delle merci non erano traducibili nei numeri odierni. I dati, infatti, mostrano che ogni anno gli spostamenti alle frontiere interne sono quasi 50 milioni, mentre i passaggi alle frontiere esterne poco più di 200 milioni[1], ma si calcola che entro il 2025 saranno 887 milioni le persone che visiteranno lo spazio Schengen.

I numeri sono considerevoli, ancor più rilevanti se incrociati con i dati relativi all'incremento della criminalità nell'area Schengen, spesso messa in correlazione proprio con l'abolizione dei controlli interni[2]. La libertà di circolazione e soggiorno all'interno dell'Unione europea sembra porsi, infatti, in un rapporto di proporzionalità diretta rispetto all'aumento di alcuni reati. Non si tratta solo di immigrazione clandestina e terrorismo, vengono in rilievo anche altre ipotesi delittuose eterogenee che includono alcuni reati contro il patrimonio (in particolare, truffa, contraffazione, riciclaggio e ricettazione), contro la persona (tratta) o la pubblica amministrazione (per lo più corruzione), nonché il traffico di sostanze stupefacenti o di armi.

Inevitabile, dunque, la ricerca di nuove modalità di controllo più efficaci e capaci di coniugare il difficile binomio sicurezza/scorrevolezza dei passaggi alle frontiere – e il conseguente sviluppo nell'ultimo decennio di tecnologie più moderne per la gestione del problema. Il riferimento riguarda l'introduzione del sistema *Intelligent portable border control system*, meglio noto come *IBorderCtrl*[3], che associa l'analisi di una grande quantità di dati

---

[1] Cfr. *www.europarl.europa.eu/doceo/document/TA-8-2017-0411_IT.pdf*. Nella Relazione introduttiva si legge «*Il flusso di passeggeri alle frontiere esterne dell'Unione europea è cresciuto e continuerà a crescere in futuro. Si prevede che nel 2025 il numero totale degli attraversamenti di frontiera regolari salga a 887 milioni, di cui circa un terzo sarebbe effettuato da cittadini di Paesi terzi che si recano nei Paesi Schengen per visite di breve durata*».

[2] Per un'analisi del binomio sicurezza e frontiere, si veda LONGO, *Identità, sicurezza, frontiere. I paradigmi della lotta alla criminalità organizzata nell'Unione Europea*, in *Meridiana*, 2002, 43.

[3] Informazioni ufficiali sull'introduzione di questa nuova tecnologia sono reperibili su

(*big data, open data, personal data*) dei passeggeri in transito con uno strumento di intelligenza artificiale addestrato al riconoscimento facciale e che costituisce un punto di approdo rispetto a politiche già avviate dall'Unione europea.

Con l'abolizione delle frontiere interne si era reso ben presto evidente che la sicurezza dello spazio Schengen potesse essere garantita solo con il rafforzamento dei controlli alle frontiere esterne e che non fosse sufficiente investire del problema i paesi frontalieri. L'adozione di normative nazionali ha spesso determinato difformità operative[4] tali da rendere necessaria, nel 2004, l'istituzione dell'Agenzia *Frontex*[5], con compiti di armonizzazione delle pratiche di controllo e di coordinamento operativo. Tuttavia, un significativo cambio di passo si è avuto nel 2016, con l'attribuzione a *Frontex* di poteri codecisionali nella gestione dei flussi migratori e con l'adozione della Direttiva 2016/681/UE relativa all'istituzione del codice di prenotazione[6]. Contestualmente, l'adozione di strumenti tra cui *Schengen Information System*, *Visa Information System* ed *Entry/Exit System*[7] ha posto l'accento sull'importanza della raccolta dei dati dei visitatori nel controllo delle frontiere e al contempo nel contrasto del crimine. Tuttavia, nessuno di questi sistemi si era spinto oltre la raccolta e l'incrocio dei dati, seppure automatizzati, mentre *IBorderCtrl* mostra tutta la sua innovatività nell'associare l'uso dei dati con l'intelligenza artificiale, sfruttandone le prestazioni e le potenzialità[8].

---

www.iborderctrl.eu.

[4] Per un'ampia bibliografia sul punto si veda *Il diritto dell'immigrazione. Profili di Diritto Italiano, Comunitario e Internazionale,* in *V quaderno de «Il diritto dell'economia»*, a cura di Gasparini Casari-Cordini, Modena, 2010, 65.

[5] Regolamento (CE) n. 2007/2004 del Consiglio del 26 ottobre 2004. Si veda *www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2004R2007:20070820:IT:PDF*. L'Agenzia è divenuta operativa il 3 ottobre 2005.

[6] Si tratta della Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio del 27 aprile 2016 *sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*, in *www.eur-lex.europa.eu/legalcontent/IT/TXT/PDF/?uri=CELEX:32016L0681&from=IT*. Il codice di prenotazione contiene (PNR) informazioni personali fornite dai passeggeri, raccolte e conservate dai vettori aerei.

[7] Per approfondimenti, si veda *www.ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders_en* e anche *www.europarl.europa.eu/factsheets/it/sheet/153/gestione-delle-frontiere-esterne*.

[8] Quella della intelligenza artificiale è una disciplina relativamente nuova, che alle difficoltà di definizio-

Questo contributo intende illustrare il funzionamento del sistema *IBorderCtrl* al fine di approfondirne i meccanismi e le capacità di sviluppo, ma anche di sottolinearne i limiti e le criticità rispetto ai sistemi normativi nazionali e sovranazionali.

2. *Breve inquadramento sugli strumenti di controllo previsti dall'Unione europea.* Le attività di controllo alle frontiere esterne dell'Unione europea hanno mostrato fin da subito la loro inadeguatezza in quanto gestite quasi esclusivamente da operatori in difficoltà per l'elevato numero delle persone in transito di cui accertare l'identità. È quindi emersa la necessità di disporre di strumenti più sofisticati e tecnologicamente avanzati, in grado di risolvere i problemi di lentezza e la fallacia dei controlli[9].

---

ne e di delimitazione dell'ambito di operatività aggiunge non poche criticità quando la si coniuga con le categorie giuridiche. L'impiego di tali sistemi, infatti, si pone spesso in contrasto con il più generale tema della tutela dei diritti fondamentali e con i principi propri della scienza penalistica. Le ragioni di un interesse penalistico per le nuove tecnologie risiedono soprattutto nell'esigenza di ricondurre a razionalità il sistema rispetto ai differenti ruoli che l'intelligenza artificiale può rivestire, e che possono tradursi in benefici per la collettività ma – al contempo – anche in pregiudizi, non solo in termini di rischio, per i beni giuridici. Sulla storia della nascita dell'intelligenza artificiale, si veda ITALIANO, *Intelligenza artificiale: passato, presente, futuro,* in *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Pizzetti, Torino, 2018, 206 ss.; RUSSELL-NORVIG, *Artificial intelligence. A modern approach*, Edimburgo, 2016. Sulle tematiche del rapporto tra diritto e nuove tecnologie, BARFIELD-PAGALLO, *Research handbook on the Law of Artificial Intelligence*, Northampton, 2018; CORASANITI, *Il diritto nella società digitale*, Milano, 2021; *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di Dorigo, Pisa, 2020; HALLEVY, *Liability for crimes involving artificial intelligence system*, Cham, 2015; IENCA, *Intelligenza. Per un'unione di intelligenza naturale e artificiale*[3], Torino, 2019; *Tecnodiritto*, a cura di Moro, Sarra, Milano, 2021; QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion,* Cham, 2020; *Intelligenza artificiale. Il diritto, i diritti l'etica*, a cura di Ruffolo, Milano, 2020; SANTOSUOSSO, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano, 2020; TAMBURRINI, *Etica delle macchine. Dilemmi morali per robotica e intelligenza artificiale*, Roma, 2020; TREZZA, *Diritto e intelligenza artificiale. Etica – Privacy – Responsabilità – Decisione*, Pisa, 2020; UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo,* in *Sist. Pen.*, 2020, 4, 2. Cfr. anche, BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *Dir. Pen. Uomo*, 2019, 9; RULLI, *Giustizia predittiva, intelligenza artificiale e modelli probabilistici. Chi ha paura degli algoritmi?* in *Analisi Giur. dell'economia*, 2018, 2, 533, MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia,* in *DiScrimen*, 2020; MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; *Diritto penale e intelligenza artificiale. Nuovi scenari*, a cura di Balbi-De Simone-Esposito-Manacorda, Torino, 2022.

[9] Alcuni Stati europei, tra cui Spagna e Germania, hanno adottato sistemi di scansione dei documenti elettronici al varco digitale, senza l'intervento di alcun operatore umano; in Germania è stato impiegato il sistema *Easy Pass*, mentre in Spagna *ABC gates*, sulla falsariga degli Stati Uniti, che utilizza già da

Il ricorso a nuove procedure ha avuto un andamento per niente lineare. Le istanze connesse al tema della sicurezza nello spazio Schengen, scaturite in particolar modo dalla necessità di contrastare i fatti di terrorismo legati soprattutto al fondamentalismo islamico, sono state ritenute prioritarie e hanno portato all'introduzione di diversi sistemi di controllo

Gli strumenti e le procedure impiegati per sorvegliare le frontiere esterne possono essere raggruppati in tre categorie, a seconda che adottino sistemi tradizionali come la verifica dei documenti, seppure automatizzata; tecniche innovative di trattamento dei dati oppure combinino, in un'azione sinergica, le nuove tecnologie.

Appartiene al primo gruppo la procedura nota come *Registered Traveller Programme* (RTP), proposta nel 2008 dalla Commissione europea, che introduce controlli agevolati dei documenti in alcuni valichi dotati di cd. *porte automatiche* per i viaggiatori registrati o frequenti[10]. Alla stessa stregua, si annoverano nel primo raggruppamento anche strumenti come il *Visa Information System* (VIS).

Nella seconda categoria, invece, si inserisce il cd. *Passenger Name Record* (PNR), che introduce l'obbligo a carico dei vettori aerei di trasferire alle autorità di contrasto degli Stati membri l'elenco di dati relativi al passeggero e al suo viaggio, a fini di prevenzione, accertamento, indagine e azione penale in caso di reati di terrorismo e di reati gravi[11]. Gli Stati possono valutare

---

tempo *Automated Passport Control*. Cfr. *Facial recognition application for border control, 2018 International Joint Conference on Neural Networks* IJCNN 2018, a cura di Carlos-Roca-Torres-Tena, Rio de Janeiro, 2018, 1-7.

[10] La possibilità di sottoporsi a controlli più rapidi è subordinata alla condizione che la maggior parte dei essi siano effettuati già prima della partenza dai Paesi terzi. Sul punto si veda *www.eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52013PC0096&from=IT*.

[11] Il sistema PNR è stato introdotto con la Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. L'allegato II della Direttiva contiene l'elenco tassativo delle fattispecie di reato per le quali è consentito il ricorso al sistema del PNR. Si tratta di 26 delitti per i quali è possibile immaginare un raggruppamento in due categorie, a seconda se prevale il carattere della maggiore gravità del fatto, piuttosto che l'aspetto di maggiore incidenza alle frontiere. Rientrano nel primo gruppo, ad esempio, alcuni reati contro la persona, come l'omicidio e la tratta o il sequestro e lo stupro, ma anche terrorismo, associazione per delinquere e alcuni reati contro la pubblica amministrazione come la corruzione. Nella seconda categoria sono annoverate molte ipotesi di falso e contraffazione, alcuni tipi di traffico (dagli organi umani, alle armi e droghe).

l'opportunità di non trattare i dati, ovvero di cederli ad altri Stati europei. È altresì regolata l'ipotesi della cessione a Paesi terzi.
Ricorre al trattamento dei dati anche l'*European Travel Information and Authorisation System* (ETIAS), che dovrebbe diventare pienamente operativo nel 2023[12]. Il sistema rilascia un'autorizzazione elettronica per l'ingresso dei cittadini di Paesi terzi esenti dall'obbligo di visto e ha lo scopo di valutare se la loro presenza nel territorio degli Stati membri possa rappresentare un pericolo per la sicurezza, in termini di immigrazione illegale o di alto rischio epidemico. La raccolta, il tracciamento e l'aggiornamento delle informazioni sui visitatori senza obbligo di visto hanno lo scopo di rendere più veloci le operazioni di controllo alle frontiere e anche di ridurre il numero di rifiuti di ingresso in Europa.
La previsione circa la possibilità di raccolta delle informazioni relative anche a voli intra-europei, così come la circostanza che siano analizzati e valutati dati relativi a viaggiatori nei cui confronti non sussistano accuse o sospetti circa la commissione di fatti penalmente rilevanti, ha imposto numerosi limiti. Queste restrizioni sono state probabilmente dettate dalla consapevolezza dei possibili rischi di violazione di diritti fondamentali, tra cui il diritto alla riservatezza. Le ipotesi di utilizzo dei dati, infatti, sono tassativamente indicate all'art. 6 del Regolamento (UE) 2018/1240 e non possono, in alcun caso, avere a oggetto informazioni sensibili come l'origine razziale o etnica, le opinioni politiche, la religione o le convinzioni filosofiche, l'appartenenza sindacale, lo stato di salute, la vita o l'orientamento sessuale dell'interessato[13]. Gli Stati sono tenuti a nominare un'autorità che funga da unità di informazione sui passeggeri, con al suo interno la figura di un responsabile della protezione dei dati. Infine, ove sia stata istituita una banca dati allo scopo di archiviare tutte le informazioni raccolte, queste non possono essere conservate per più di cinque an-

[12] Regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226.
[13] Qualora un'unità di informazione nazionale riceva dati PNR che rivelano tali informazioni, questi sono cancellati immediatamente. Cfr. art. 13 co. 4. L'allegato I elenca diciannove tipologie di dati che possono essere oggetto di raccolta ai sensi della Direttiva (UE) 2016/681, e anche in tale caso si tratta di un'elencazione tassativa.

ni[14].

Il già collaudato *Schengen Information System* (SIS II) – introdotto nel 2006 e rivisitato a mezzo di tre Regolamenti approvati nel 2018, finalizzato alla raccolta di dati e segnalazioni da parte di tutti i Paesi membri su persone o cose che costituiscono una minaccia per l'ordine pubblico o la sicurezza nazionale – è stato affiancato dal sistema basato su un codice di prenotazione[15].

Lo *Schengen Information System* II si fonda, dunque, sia sulla condivisione di informazioni relative a specifiche categorie di soggetti e oggetti, sia sulla raccolta di dati biometrici. In particolare, è una banca dati che contiene le segnalazioni[16] di cittadini di Paesi terzi cui è opportuno negare l'ingresso in Europa e di persone scomparse; l'elenco di oggetti collegati alla commissione di reati, le informazioni circa l'immatricolazione di veicoli, e, soprattutto, le impronte palmari e digitali, le immagini facciali e campioni di DNA. L'intento sotteso all'uso congiunto dei due strumenti è duplice, consistendo nella condivisione del maggior numero possibile di informazioni tra gli Stati, da un lato, e nell'impedimento alla libera circolazione nello spazio Schengen di soggetti dediti al crimine, dall'altro.

Sin qui il sistema di controllo appare come una raccolta e un'analisi dei dati, se non fosse che, contestualmente, l'Unione europea ha presentato, nel 2017, *Entry/Exit System* (EES) quale nuovo e ulteriore sistema informativo centralizzato, finalizzato alla registrazione degli ingressi e delle uscite ai varchi frontalieri dei cittadini extracomunitari e fondato anch'esso sulla raccolta dei dati biometrici[17]. Proprio quest'ultima caratteristica permette di inserire EES nel terzo gruppo, comprendente le azioni che sfruttano tecniche all'avanguardia, anche partendo da sistemi annoverabili nelle categorie precedenti. La proce-

[14] Cfr. *www.consilium.europa.eu/it/policies/light-against-terrorism/passenger-name-record/*.

[15] Si tratta dei Regolamenti (UE) 2018/1860 per il rimpatrio di cittadini di Paesi terzi il cui soggiorno è irregolare; 2018/1861 nel settore delle verifiche di frontiera; 2018/8162 nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, tutti entrati in vigore il 28 dicembre 2019 e pienamente operativi da dicembre 2021. Per maggiori approfondimenti sul funzionamento del SIS II, si veda *www.eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM%3Al14544*

[16] Anche in questo caso la rilevanza delle segnalazioni ha natura tassativa e le diverse ipotesi sono previste nel Regolamento (CE) n. 1987/2006 e nella Decisione 2007/533/GAI.

[17] Il sistema è operativo dal 2020 ed è stato introdotto dal Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio del 30 novembre 2017. Si veda *www.eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri= CELEX:32017R2226&qid=1517412828916&from=en*

dura automatizza l'apposizione del timbro sul passaporto utilizzando i dati raccolti dal VIS, le informazioni sulle impronte digitali provenienti dalla banca dati *European Dactyloscopie* (EURODAC) e le segnalazioni presenti nell'*European Criminal Records Information System* (ECRIS)[18]. Permette, inoltre, di combinare sia dati alfanumerici, sia dati biometrici composti da quattro impronte digitali e dall'immagine del volto.

Il sistema costituisce l'evoluzione di quanto già presentato nel 2013 nel cd. pacchetto *Frontiere intelligenti*, che aveva sollevato numerose criticità in merito alla tutela della *privacy*. Il Garante europeo della protezione dei dati, infatti, aveva ritenuto che la conservazione di una grande mole di dati personali e biometrici non fosse proporzionata agli scopi perseguiti, e aveva evidenziato un contrasto con i principi della Carta europea in tema di tutela del diritto alla vita privata e familiare, nonché di tutela della protezione dei dati personali[19].

Alcune modifiche sono state apportate al sistema per superare i rilievi mossi dal Garante[20]. Gli obiettivi perseguiti sono stati considerati di fondamentale importanza, ma le misure adottate[21] sono state ritenute non sufficienti a garantire la sicurezza dello spazio Schengen, rispetto soprattutto alla minaccia del terrorismo. Sono stati così ulteriormente incrementati gli strumenti di controllo, nel tentativo di identificare tutte le categorie di soggetti che attraversano le frontiere europee.

Con ogni probabilità, lo sviluppo tecnologico e l'implementazione dei sistemi di intelligenza artificiale hanno costituito l'ulteriore spinta all'introduzione – seppure in via sperimentale – del nuovo sistema *IBorderCtrl*, che, per le sue

---

[18] Si tratta del casellario giudiziale europeo istituito nel 2012, che permette agli Stati membri di scambiarsi in tempo reale informazioni digitalizzate circa le condanne registrate nei casellari dei singoli paesi. Cfr. *www.e-justice.europa.eu/content_taking_into_account_previous_convictions-95-it.do*

[19] *Cfr. www.edps.europa.eu/sites/default/files/publication/13-07-18_smart_borders_ex_sum_it.pdf*

[20] L'elenco dei dati da sottoporre alla registrazione, ad esempio, è stato ridotto da 36 a 26. Il Garante, nella consapevolezza che il raggiungimento di obiettivi di rilevante interesse pubblico spesso determina una legislazione contraddittoria, ha invitato a osservare le linee guida dettate in materia. La valutazione del rispetto dei criteri di necessità e proporzionalità, infatti, comporta una «*minimizzazione del conflitto tra le diverse priorità*». Si veda GUIDA-TOZZI, *La valutazione della proporzionalità delle misure che limitano i diritti fondamentali della privacy nelle nuove linee guida del garante europeo della protezione dei dati,* in *www.ejplt.tatodpr.eu/Article/Archive/index_html?ida=185&idn=6&idi=-1&idu=-1*, 1/20

[21] Per una panoramica più dettagliata delle misure adottate, si veda *www.eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52016DC0205&from=EN*

caratteristiche, si inserisce anch'esso nel terzo gruppo delle misure poste a controllo delle frontiere europee.

3. *Un significativo cambio di passo.* La crescente centralità dei temi legati alla sicurezza nell'agenda europea scaturisce sia da fattori contingenti e reali, sia dalla paura e dalla incertezza per il futuro. Si assiste, da un lato, all'affinamento delle strategie criminali per il superamento dei confini europei e all'aumento dei flussi migratori, con una crescente consapevolezza sulle possibilità di manipolazioni e alterazioni dei dati e dei documenti, anche grazie alla criminalità informatica. Dall'altro, si registra anche un rafforzamento del dominio della paura – la cd. fobocrazia – che sin ora era stata contenuta nei singoli confini nazionali.
Le conseguenze tangibili sono duplici: il ripristino di fatto delle frontiere, con la reintroduzione dei controlli anche per i cittadini europei a opera del Regolamento (UE) 2017/458[22], e il ricorso massivo alle tecniche di riconoscimento facciale, sin ora considerate sproporzionate rispetto agli obiettivi perseguiti.
Se questo è il quadro di riferimento in cui si inserisce *IBorderCtrl*, il suo fondamento coincide con la considerazione che, preso singolarmente, ogni sistema, anche quello più avanzato, può portare a risultati erronei. L'impronta può essere manipolata, la faccia camuffata, ma finanche lo *scanner* della vena del palmo della mano, sinora ritenuto più efficace del rilevamento delle impronte, può subire alterazioni a causa di fattori esterni. Solo la combinazione di tutti gli strumenti a disposizione è in grado di garantire un miglior risultato riguardo agli obiettivi di controllo e di monitoraggio delle frontiere[23].
La nuova procedura costituisce una novità assoluta perché sfrutta più tecniche contemporaneamente: dati personali, dati biometrici[24], riconoscimento faccia-

[22] Il Codice Schengen, istituito con Regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio del 9 marzo 2016, che istituisce un codice unionale relativo al regime di attraversamento delle frontiere da parte delle persone (Codice frontiere Schengen), è stato sospeso numerose volte (si calcola siano 116. Si veda *www.ispionline.it/it/pubblicazione/europa-blindata-25410*), sia per esigenze connesse agli attacchi terroristici, sia, recentemente, per esigenze sanitarie connesse alla pandemia in atto.
[23] CROCKETT-O'SHEA-SZEKEL-MALAMOU-BOULTADAKIS-ZOLTAN, *Do Europe's borders need multi-faceted biometric protection?* in *Biometric Technology Today,* 2017, 7, 1.
[24] L'art. 9 del Regolamento (UE) 2016/679, meglio noto come GDPR, include nei dati personali anche i dati biometrici; tuttavia, in questa analisi li si tratta separatamente, in considerazione del diverso momento in cui vengono trattati.

le, tecnica di rilevamento dell'inganno. Il sistema prevede due fasi, una antecedente l'inizio del viaggio e una contestuale all'attraversamento della frontiera.

La prima, finalizzata a valutare un complessivo grado di rischio rispetto all'eventualità che il viaggiatore ponga in essere condotte criminose una volta entrato nello spazio Schengen, è incentrata sull'ottenimento di informazioni sia sulla persona sia sui dettagli del viaggio e prende le mosse da alcuni obblighi posti a carico del soggetto. Qualche giorno prima della data effettiva del viaggio, egli è tenuto a preregistrarsi sulla piattaforma digitale dedicata, allegando una semplice fotografia e indicando alcune informazioni personali. Dopo aver espletato tali attività, il soggetto dovrà sottoporsi a una intervista condotta da una guardia virtuale di frontiera, una sorta di *avatar*.

Questo sistema, che erroneamente viene definito ora come una semplice forma di riconoscimento facciale, ora come un rilevatore automatico di inganno, combina invece entrambi gli aspetti con una forma di intelligenza artificiale addestrata, tramite il *machine learning*, a elaborare tutti i dati raccolti e accertare la veridicità dei dati forniti[25].

L'*avatar*, con sembianze umane personalizzate, create per mettere a proprio agio ogni singolo viaggiatore, interroga l'utente sui motivi del viaggio. Nello specifico, le domande elaborate sono sedici. Il contenuto non può essere conosciuto in anticipo, in quanto l'algoritmo ha un potere di scelta autonomo sulle domande da rivolgere. L'*avatar* adatta le domande sia alle risposte fornite di volta in volta sia al profilo dell'intervistato, assumendo anche un certo tipo di comportamento per favorire la raccolta di informazioni utili.

La nuova tecnologia ha il compito di verificare la veridicità delle risposte, incrociando i dati caricati sulla piattaforma dallo stesso viaggiatore tanto con quelli contenuti nelle banche dati istituzionali poste in rete tra loro (eventuali condanne penali, inserimento del nome in liste nere o segnalazioni di altro genere), quanto con una serie di *open data* raccolti nel *web*.

Tuttavia, il sistema è chiamato anche a valutare l'attendibilità della persona e

[25] Il sistema adotta la tecnologia elaborata dal Dipartimento di Calcolo Computazionale e Matematica della *Manchester Metropolitan University*, denominata *Silent Talker*. Si veda *www.mmu.ac.uk/news-and-events/news/story/?id=77*.

una sua eventuale condotta ingannevole: non sono solo le risposte fornite e le eventuali contraddizioni verbali a permettere alla macchina di accertarne la verità, bensì il complesso del comportamento non verbale rilevato. A differenza delle comuni macchine delle verità, *IBorderCtrl* è uno strumento di intelligenza computazionale, il cui apprendimento è fondato sulla generalizzazione di esempi ingannevoli ed è indipendente da un modello esplicativo sottostante. Ciò permette di esaminare i micro-gesti e di combinare autonomamente i singoli indicatori, prescindendo dall'analisi degli indicatori fisiologici e delle micro-espressioni del viso, riuscendo a decifrare le emozioni dell'intervistato tramite l'analisi della mimica facciale, senza che il soggetto riesca a correggere e controllare psicologicamente queste manifestazioni.

A seguito di questa procedura viene assegnato un punteggio di rischio[26], che sarà consegnato alle guardie di frontiera preposte al controllo da svolgersi nella seconda fase. Si tratta di una sorta di *screening* digitale pre-partenza che, in linea con gli scopi perseguiti dai sistemi illustrati in precedenza (ad esempio EES), permette di migliorare in termini di efficienza il controllo e ridurre i tempi di attesa alle frontiere.

La seconda fase, infatti, risulta più veloce e incentrata su un vero e proprio sistema di riconoscimento facciale volto ad accertare l'identità del soggetto che intende oltrepassare il confine. La guardia di frontiera dispone di una unità portatile che le permette di raccogliere tutti i dati biometrici utili alla verifica dell'identità, come il sensore di impronta digitale e palmare, la fotocamera e il lettore di documenti. Nello specifico, la sovrapposizione delle immagini, raccolte con il dispositivo portatile, a quelle contenute nei documenti; l'abbinamento dell'immagine con il modello biometrico della persona e le sequenze video permettono la verifica della corrispondenza dell'identità di colui che ha effettuato la registrazione nella prima fase con la persona che si trova al valico, determinando il suo riconoscimento come utente *IBorderCtrl*. Effettuata la verifica dell'identità della persona, la guardia di frontiera – coadiuvata dalla valutazione del rischio elaborata dall'*avatar* – decide se auto-

[26] Per comprendere le motivazioni del punteggio di rischio assegnato è possibile rivolgere una richiesta di accesso agli atti a *EuroDynamics*, la società capofila del progetto. Si veda *www.eurodyn.com/?s=iborderctrl*.

rizzare l'ingresso del viaggiatore nell'area Schengen o sottoporlo a un controllo più approfondito, a seguito del quale l'autorizzazione a varcare i confini può anche essere negata.

Gli studi condotti circa l'efficacia dello strumento riportano un *true positive rate* pari al 95,3%, un *false positive rate* dello 0,1% e un'accuratezza complessiva del 99,5%, risultati che soddisfano pienamente i requisiti richiesti nelle linee guida elaborate per il sistema *Frontex*[27].

La sperimentazione è durata tre anni e il sistema è stato impiegato ai controlli frontalieri di Ungheria, Lettonia e Grecia da settembre 2016 ad agosto 2019, grazie al finanziamento di 4,5 milioni di euro stanziati dal programma di ricerca della Commissione europea *Horizon 2020*[28].

4. *IBorderCtrl: verso nuove misure di prevenzione?* In tema di regolamentazione degli ingressi nell'area Schengen da parte di cittadini extracomunitari, il quadro normativo di riferimento va ricercato sia nelle fonti di diritto sovranazionale sia nelle singole legislazioni nazionali.

Il provvedimento di autorizzazione al passaggio della frontiera a seguito del superamento delle procedure previste da *IBorderCtrl* si aggiunge a quello che si ottiene con il rilascio del visto, ovvero costituisce l'unica autorizzazione per coloro che rientrano nelle categorie esentate dall'obbligo di visto.

Alla stessa stregua del provvedimento di visto, non si può negare la natura formale di atto pubblico – nella specie amministrativo[29] – all'atto di diniego

---

[27] Cfr. *www.IBorderCtrl.eu*; si veda anche *www.eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020XC0417(07)&from=IT*.

[28] Tale progetto di ricerca, finanziato attraverso il programma Horizon 2020, ha strutturato il sistema *IborderCtrl* come tecnologia in grado di accelerare i processi di attraversamento delle frontiere, migliorando la sicurezza e la fiducia nei confronti dei controlli di frontiera. Al progetto, coordinato dall'*European Dynamics Luxembourg Sa*, ente privato con scopo di lucro, hanno partecipato dodici *partner*s, tra i quali enti di ricerca (*Erevnitiko Panepistimiako institouto systimaton epikoinonion kai ypolgistonempr, Kentro Meleton Asfaleias*), università (T*he Manchester Metropolitan University; Gottfried Wilhelm Leibniz Universitaet Hannover*), enti pubblici (*Orszagos Rendor –Fokapitanysag; Komenda Glowna Strazy Granicznej; Latvian State Border Guard*) e numerose società private con scopo di lucro (*Stremble Ventures Ltd; Itti Sp Zoo; Everis Aeroespacial y Defensa Sl; Biosec Group Korlatolt Felelossegu Tarsasag; Jas Technologie Spolka z Ograniczona Odpowiedzialnoscia; Hellenic Train - Anonymi Sidirodromiki Etaireia*). Per consultare i risultati del progetto di ricerca, ad oggi concluso, si v. *www.cordis.europa.eu/project/id/700626/it*.

[29] Sul punto si veda BALBI, *Le tipologie sanzionatorie: la prevenzione personale, le misure di prevenzione personali*, in *Riv. it. dir. proc. pen.*, 2017, 2, 4.

con cui la guardia di frontiera impedisce l'ingresso a seguito di un elevato punteggio di rischio assegnato dall'intelligenza artificiale, con la conseguenza che il viaggiatore respinto potrà esperire gli ordinari mezzi di impugnazione previsti nell'ambito della giurisdizione amministrativa.

Il sistema *IBorderCtrl*, fondamentalmente basato su una valutazione di pericolosità, evidenzia alcune criticità, come ad esempio l'elaborazione mediante un sistema computazionale del tutto automatizzato della valutazione di pericolosità.

L'obiettivo sotteso al funzionamento della nuova procedura di controllo è dichiaratamente quello di prevenire la commissione di reati nell'area Schengen da parte di soggetti extracomunitari. Dunque, una finalità di prevenzione del crimine che richiede una valutazione di pericolosità su cui fondare, eventualmente, un provvedimento interdittivo. Ritorna, così, quel concetto di prevenzione declinato in diverse forme nel nostro ordinamento e posto a tutela di beni di particolare rilevanza, che sembra echeggiare i tratti tipici delle misure di polizia prima e di quelle di prevenzione poi, riproponendo una serie di problemi irrisolti[30].

Anche nel caso di *IBorderCtrl* si prescinde dall'accertamento di un fatto di reato, il che sarebbe, di per sé, sufficiente a muovere le stesse obiezioni sollevate in dottrina[31] in tema di misure di prevenzione personali.

---

[30] In relazione ai rilievi critici sollevati dalla dottrina in merito alle misure di prevenzione personali e ancora irrisolti, si rimanda senza pretesa di esaustività a MAIELLO, *Profili sostanziali: le misure di prevenzione personali*, in *Giur. it.*, 2015, 1523 ss; MARTINI, *Essere pericolosi. Giudizi soggettivi e misure personali*, Torino, 2017; BERTOLINO, *Diritti fondamentali e diritto penale della prevenzione nel paradigma dell'efficienza*, in *La pena, ancora: fra attualità e tradizione. Scritti in onore di Emilio Dolcini*, a cura di Paliero-Viganò-Basile-Gatta, Torino, 2018, 847 ss.; v. il numero speciale della Rivista italiana di diritto e procedura penale del 2017, fascicolo 2 che pubblica gli *Atti del V Convegno nazionale dell'Associazione Italiana dei Professori di Diritto Penale, Milano, 18/19 novembre 2016*, dedicato a *Delle pene senza delitto.* In particolare, v. i contributi di BALBI, *Le misure di prevenzione personali*, 505 ss; CATENACCI, *Le misure personali di prevenzione tra 'critica' e 'progetto': per un recupero dell'originaria finalità preventiva*, 526; LACCHÈ, *Uno 'sguardo fugace'. Le misure di prevenzione tra Ottocento e Novecento*, 413 ss.; MARTINI, *Il mito della pericolosità. Alla ricerca di un senso compiuto del sistema della prevenzione personale*, 536 ss.; MAGI, *Sul recupero di tassatività nelle misure di prevenzione personali. Tecniche sostenibili di accertamento della pericolosità*, 490 ss.; PELISSERO, *I destinatari della prevenzione* praeter delictum*: la pericolosità da prevenire, la pericolosità da punire,* 439.

[31] Tra i contributi più recenti in tema di misure di prevenzione personali si veda AMARELLI, *Ulteriormente ridotta la tipicità del delitto di violazione degli obblighi inerenti alla misura di prevenzione: per la Cassazione anche il divieto di partecipare a pubbliche riunioni contrasta con il principio di determinatezza*, in *Dir. pen. cont.*, 2018, 7-8, 174 ss.; BALBI, *Le tipologie*, cit., 1 ss.; CERESA-GASTALDO, *Misure*

Siamo nella stessa logica che ha da sempre contraddistinto le misure di prevenzione personali, utilizzate dagli Stati "per affrontare in chiave repressiva ma con forma 'preventiva', un vasto insieme di dati sintomatici di sospetto, comportamenti devianti, semplici forme di disobbedienza, di 'anormalità', di disordini e rischi"[32]. Ieri i rischi erano avvertiti provenire da mendicanti e vagabondi, poi via via dagli oziosi, dalle persone pericolose per l'ordine nazionale, dagli immeritevoli di ogni riguardo sotto il profilo morale e sociale, dalle classi pericolose, dalle classi meno abbienti, da coloro che minacciano la proprietà e la stabilità, dagli anarchici, dagli antifascisti, dai terroristi, dai mafiosi[33]... Oggi l'opera di contenimento è fatta nei confronti dei migranti, visti sostanzialmente come una minaccia all'ordine e al benessere della civiltà occidentale.

L'Europa si difende saggiando possibilità di controllo che spostino ancora più indietro il momento in cui è possibile intervenire in via preventiva. Una scelta di politica criminale molto risalente nella storia, chiara ma mimetizzata perché effettuata non sotto i riflettori del diritto penale, ma nel raggio d'azione dei controlli di frontiera. Questo sulla base dell'idea che lo Stato non può difendersi soltanto a reato commesso, ma deve difendere sé stesso, la società e i cittadini anche da "pericoli non immediati", facendo a meno del 'fardello' dei principi posti a presidio delle libertà fondamentali. Se questi sono alcuni tratti caratteristici, e costanti, delle misure di prevenzione, le critiche non possono che amplificarsi nel caso di *IborderCtrl.* In questa ipotesi si ha, lo dicevamo, una ulteriore anticipazione del momento valutativo della pericolosità del sog-

---

di prevenzione e pericolosità sociale: l'incolmabile deficit di legalità della giurisdizione senza fatto, in *Dir. pen. cont.*, 3/12/2015; FIANDACA, (voce) *Misure di prevenzione (profili sostanziali)*, in *Dig. Disc. Pen.*, vol. VIII, Torino, 1994, 110 ss.; GRASSO, *Le misure di prevenzione personali e patrimoniali nel sistema costituzionale*, in *www.sistemapenale.it*, 14 febbraio 2020; MAIELLO, *De Tommaso c. Italia e la cattiva coscienza delle misure di prevenzione*, in *Dir. pen. proc.*, 2017, 8, 1039 ss.; MENDITTO, *La sentenza De Tommaso c. Italia: verso la piena modernizzazione e la compatibilità convenzionale del sistema della prevenzione*, in *Dir. pen. cont.*, 2017, 4; MOCCIA, *Le misure di prevenzione: un esempio paradigmatico di truffa delle etichette*, in *www.penaledp.it*, 11 gennaio 2021; PELISSERO, *Le misure di prevenzione*, in *www.discrimen.it*, 13 febbraio 2020; PULITANÒ, *Relazione di sintesi. Misure di prevenzione e problema della prevenzione*, in *Riv. it. dir. proc. pen.*, 2017, 2, 637 ss.; VIGANÒ, *La Corte di Strasburgo assesta un duro colpo alla disciplina italiana delle misure di prevenzione personali*, in *Dir. pen. cont.*, 2017, 3, 296 ss.

[32] V. LACCHÈ, *Uno sguardo fugace*, cit., 419 ss.

[33] V. BALBI, *Le misure*, cit., 516; PELISSERO, *I destinatari*, cit., 443 ss.

getto, fondata esclusivamente su un giudizio di natura predittiva totalmente disancorato da qualsiasi violazione di legge, foss'anche in termini di "mero sospetto" come invece accade nelle – già estremamente problematiche - misure di prevenzione. *IBorder* non comporta effetti desocializzanti, propri di tutte le misure di prevenzione[34], perché non ne ha la possibilità, ma pregiudica in radice qualsiasi *chance* di possibile integrazione: interviene a 'difendere' la società europea da qualsiasi tipo d'impatto col soggetto ritenuto predittivamente 'pericoloso', impedendogli *tout court* l'accesso negli spazi che essa occupa. Il risultato è noto (ma i suoi contorni ancor più arbitrari ed inquietanti): comprimere le libertà sulla base di una mera inferenza statistica.

Il provvedimento di diniego all'ingresso del viaggiatore si colloca, in sintesi, in un'area grigia che esula dalle tutele proprie del diritto penale sostanziale e processuale[35].

I timori legati all'uso esclusivo della IA potrebbero essere ridotti in considerazione della circostanza che la decisione di autorizzare o meno l'ingresso del soggetto spetta comunque alla guardia di frontiera. Tuttavia, nell'applicazione concreta, si può immaginare – nella totale assenza di dati accessibili - che difficilmente l'operatore umano si discosterà dalla valutazione effettuata dall'*avatar*, quantomeno per non assumersi una peculiare responsabilità.

Resta aperta la questione della durata della misura. Nel nostro ordinamento, le misure di prevenzione, con tutti i limiti che le connotano, hanno tuttavia una durata massima[36]. Nel caso del provvedimento di diniego a entrare nello spazio Schengen, nulla è detto circa la possibilità che il viaggiatore riesca poi a ottenere successivamente l'autorizzazione. Certo, può partecipare *ad libitum*

[34] Cfr. BALBI, cui si rimanda per l'inquadramento generale e i profili di illegittimità dell'istituto, *Le misure*, cit., 510 s.

[35] La valutazione della pericolosità così come il cd. *risk assessment* sono concetti, nati a inizio '900 con la scienza criminologica, che supportano l'attività giudiziale ma anche quella di *intelligence*. Nella valutazione sulla pericolosità di un reo che ha chiesto l'ammissione a una misura alternativa, ad esempio, il giudice non predice il futuro comportamento del soggetto, ma applica una probabilità statistica che ha una base fattuale, fondata sia su indicatori di tipo normativo sia sugli elementi che legano il fatto commesso alla condotta del reo.

[36] Il d. lgs. n. 159/2011 prevede un limite massimo di cinque anni, mentre la L. n. 161/2017 prevede che per il soggetto ristretto in carcere a seguito di una misura cautelare, ovvero dopo una sentenza di condanna, la misura di prevenzione sia sospesa e, superati i due anni, il giudice è tenuto a verificare la persistenza della pericolosità sociale.

alla procedura prevista da *IBorderCtrl*, ma una valutazione di pericolosità che – ad esempio – lo etichetti come un probabile, futuro terrorista, difficilmente potrebbe essere sovvertita, perché gli algoritmi, tutto sommato, hanno una loro coerenza.

Rispetto, poi, alla tipologia di soggetti a cui l'algoritmo può assegnare un elevato punteggio di rischio, nulla è detto nei documenti descrittivi del progetto che ha realizzato *IBorderCtrl*, dove si fa soltanto riferimento, e in termini meramente esemplificativi, ad alcune gravi fattispecie di reato. Diversamente, nel nostro ordinamento le categorie di soggetti a cui possono essere applicate le misure di prevenzione sono elencate tassativamente nel d. lgs. n. 159/2011[37]. Anche così, peraltro, con un più elevato *standard* di precisione, la Corte europea ha ritenuto la disciplina italiana in materia sprovvista di *una base legale sufficientemente determinata*[38]. Obiezione, dunque, che a maggior ragione va rivolta a *IBorderCtrl*.

Invero non sfugge che, trattandosi di uno strumento che è stato considerato non rientrare nella materia penale, le garanzie e le tutele previste per gli istituti di matrice penalistica sembrerebbero non doversi applicare, alla stessa stregua di quanto si è ritenuto per le misure di prevenzione personali previste dal nostro ordinamento. Ma se la dottrina oggi dubita fortemente della loro estraneità all'ambito della materia penale, analogamente il nuovo sistema di controllo alle frontiere, alla luce dell'impatto sulla libertà e sulla vita delle persone che esso comporta, fa emergere la necessità di una verifica dei suoi possibili punti di frizione con i principi fondamentali.

---

[37] Per un'ampia disamina, si veda BALBI, *Le tipologie*, cit., 8 ss.

[38] Cfr. Corte EDU [GC], 23 febbraio 2017, De Tommaso c. Italia. Fra i numerosi commenti della dottrina, si vedano: BASILE, *Tassatività delle norme ricognitive della pericolosità nelle misure di prevenzione: Strasburgo chiama, Roma risponde*, in *www.penalecontemporaneo.it,* 20 luglio 2018; DE BLASIS, *Oggettivo, soggettivo ed evolutivo nella prevedibilità dell'esito giudiziario tra giurisprudenza sovranazionale e ricadute interne*, in *Dir. pen. cont.*, 2017, 4, 128 ss.; DOLSO, *Le misure di prevenzione tra giurisprudenza costituzionale e giurisprudenza della Corte europea dei diritti dell'uomo*, in *Arch. pen.*, 2017, 3; MAGI, *Per uno statuto unitario dell'apprezzamento della pericolosità sociale. Le misure di prevenzione a metà del guado?*, in *www.penalecontemporaneo.it,* 13 marzo 2017, 135 ss.; FINOCCHIARO, *Ancora in tema di ricadute della sentenza De Tommaso. Una pronuncia del Tribunale di Monza su misure di prevenzione e fattispecie di pericolosità 'qualificata'*, 2018, 2, 197 ss.; MAUGERI, *Misure di prevenzione e fattispecie a pericolosità generica: la Corte europea condanna l'Italia per la mancanza di qualità della "legge", ma una rondine non fa primavera*, in *www.penalecontemporaneo.it,* 6 marzo 2017, 15 ss.; MENDITTO, *Misure di prevenzione e Corte europea, in attesa della Corte costituzionale*, in *www.penalecontemporaneo.it,* 22 ottobre 2018; VIGANÒ, *La Corte di Strasburgo,* cit., 370 ss.

L'assenza di un puntuale e tassativo catalogo di reati, se questa dovesse poi essere la strada seguita dal legislatore (europeo o nazionale), a cui collegare il diniego di ingresso sembra replicare, come già detto, il modello normativo censurato dalla Corte europea, con evidenti ricadute sul principio di legalità[39].
Al riguardo, però, già in materia di misure di prevenzione personali, la Corte costituzionale ha ribadito ancora una volta che, non perseguendo unicamente uno scopo afflittivo, ma soprattutto uno scopo di controllo, esse non rientrano nell'ambito di operatività del principio di legalità *ex* art. 25 Cost.[40].
Tuttavia, il quadro normativo di riferimento, peccando di genericità e indeterminatezza a cominciare dalla tipologia di pericolosità, che non è specificata, non reggerebbe neanche alle altre obiezioni poste dai giudici della Corte di Strasburgo nella decisione *De Tommaso c. Italia* del 2017[41]. Viene infatti qui in rilievo quella stessa pericolosità per la quale la Corte, in relazione alle misure di prevenzione, ha ritenuto che non siano chiari gli elementi di fatto[42] e i comportamenti specifici, la cui vaghezza potrebbe determinare ancor più applicazioni arbitrarie del sistema di controllo alle frontiere. Potrebbe difettare anche il requisito dell'attualità, che è invece elemento essenziale delle misure di prevenzione[43], dal momento che le informazioni raccolte dall'algoritmo, anche nel *web*, possono essere totalmente diacroniche.
In ogni caso, rispetto al concetto di pericolosità, la Corte costituzionale[44] ha

---

[39] Sul punto, si veda *infra,* nota 41.
[40] Così Corte cost., sentenza 27 febbraio 2019 n. 24. Sul punto in dottrina si veda PELISSERO, *Le misure*, cit., 1 ss.
[41] V., anche nell'ambito delle dinamiche tra le Corti, quanto deciso dalla Corte costituzionale in materia di misure di prevenzione in Corte cost., 24 gennaio 2019 (dep. 27 febbraio 2019), n. 24 e Corte cost., 24 gennaio 2019 (dep. 27 febbraio 2019), n. 25. Sul punto FINOCCHIARO, *Due pronunce della Corte Costituzionale in tema di principio di legalità e misure di prevenzione a seguito della sentenza De Tommaso della Corte Edu*, in *www.penalecontemporaneo.it*, 4 marzo 2019; PELISSERO, *Gli effetti della sentenza De Tommaso sulla disciplina delle misure di prevenzione dopo le recenti posizioni della Corte costituzionale*, in *Studium iuris*, 2019, 10, 1148 ss.; MAIELLO, *Gli adeguamenti della prevenzione* ante delictum *nelle sentenze costituzionali nn. 24 e 25*, in *Dir. pen. proc.*, 2020, 1, 107 ss.
[42] Cfr. PELISSERO, *Le Misure,* cit., *5*, secondo cui «*si tratta di strumenti duttili di controllo: duttilità, anzitutto, della base indiziaria che ne consente l'applicazione e che non viene meno nonostante il richiamo, introdotto sin dal 1988, alla necessità che a fondamento della misura vi siano "elementi di fatto"*».
[43] Cass., Sez. un., 4 gennaio 2018, n. 111.
[44] Così Corte cost., 27 febbraio 2019, n. 24. Tempo addietro (Corte cost., 23 marzo 1964, n. 23) la stessa Consulta aveva affermato che il mero sospetto si supera tramite una valutazione oggettiva dei fatti. Se volessimo applicare il *dictum* a *IBorderCtrl*, andrebbe notato che mancherebbero elementi di fatto sufficientemente valutabili.

recentemente affermato l'illegittimità di alcune misure di prevenzione previste dal d. lgs. n. 159/2011, che trovavano applicazione per soggetti abitualmente dediti a traffici delittuosi, a causa del riferimento a una pericolosità generica, seppure fondata su elementi di fatto.

5. *I possibili contrasti con i principi fondamentali.* La sinergia degli strumenti e delle tecniche di ultima generazione posti al servizio del controllo frontaliero allo scopo di garantire la sicurezza dell'Unione, pur essendo in grado di assicurare una migliore strategia di prevenzione e contrasto alla criminalità, non è scevra da rischi significativi in termini di violazione sia dei principi fondamentali sia dei diritti umani.

Negli ultimi anni le istituzioni sovranazionali hanno mostrato di esserne ben consapevoli, adottando alcuni importanti provvedimenti, tra cui la Proposta di Regolamento sull'approccio europeo all'intelligenza artificiale del 21 aprile 2021[45]. La logica securitaria sembra tuttavia prevalere, tanto che *IBorderCtrl* è stato introdotto in via sperimentale proprio per ridurre il rischio di entrata di persone che potrebbero commettere reati gravi. Infatti, anche se nel sistema *IborderCtrl* tutti i viaggiatori sottoposti alla misura sono considerati in buona fede[46], sussiste, tuttavia, una presunzione implicita di irregolarità, che scaturisce dall'impiego di dati biometrici (in particolar modo informazioni riguardanti la razza, l'etnia, il genere) che potrebbero essere viziati dai pregiudizi[47] riversati dall'operatore nelle macchine, in virtù delle tecniche di apprendimento automatico i cui effetti distorsivi possono determinare forme di disu-

[45] Le tappe più significative di questo approccio sono costituite dapprima dalla Strategia europea sull'intelligenza artificiale resa pubblica nel 2018, poi dalle linee guida emanate nel 2019 e, infine, dal *Libro Bianco sull'intelligenza artificiale* pubblicato dalla Commissione nel 2020. In questo arco temporale si sono susseguite anche altre iniziative (per esempio, in ambito civilistico, si segnala la *Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*), tutte a corredo dei documenti citati e di cui restituisce uno sguardo di insieme LA VATTIATA, *Brevi note 'a caldo' sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale,* in *Dir. Pen. Uomo*, 2021, 6, 1 ss. Si veda, altresì, *www.temi.camera.it/leg18/post/OCD15_14416/il-nuovo-approccio-europeo-all-intelligenza-artificiale.html*.

[46] La presunzione di buona fede è espressamente prevista nei documenti relativi al progetto *IBordeCtrl* rinvenibili in *www.iborderctrl.eu*.

[47] Sul tema v. SURDEN, *Artificial intelligence and Law: an overview*, in *Georgia State University Law Review*, 2019, 35, 1335.

guaglianza e discriminazione[48]. Ne derivano elevati rischi di criminalizzazione che potrebbero autoavverarsi, in quanto, laddove il sistema fosse alimentato da dati viziati *ab origine*, il pregiudizio sarebbe rinforzato ancora di più, inducendo a presumere la realizzabilità di reati relativamente a determinate tipologie di soggetti, con gravi pericoli di distorsione del sistema[49].

Inoltre, in assenza di una condotta che determini anche solo un pericolo per il bene giuridico tutelato, trattandosi di una mera valutazione del rischio criminale incentrata su dinamiche di massima anticipazione, si pongono problemi non solo di offensività ma anche di materialità. La logica è simile a quella sottesa ai reati ostativi, laddove le false dichiarazioni rilasciate in sede di intervista potrebbero essere intese come un indice per la commissione di futuri reati.

D'altra parte, l'esserci alla base del sistema la presumibilità di una futura commissione di reati richiama alla memoria la *ratio* sottesa ai reati di mero sospetto[50].

Ancora, i dati raccolti in archivi non istituzionali pongono ulteriori, evidenti questioni di affidabilità.

Nel contempo, si pone il problema se mentire all'*avatar* o fornire false informazioni sulla piattaforma in fase di preregistrazione possano considerarsi

---

[48] Si veda QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente riflessione tra scienze penale e informatiche*, in *www.lalegislazionepenale.eu*, 18 dicembre 2018, 6; SIGNORATO, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. proc. pen.*, 2020, 2, 612; SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro della libertà*, in *BioLaw Journal – Riv. BioDir.*, 2019, 1, 84. È stato, ad esempio, osservato che i dati immessi nel sistema riguardano solo le caratteristiche di soggetti europei e che questo costituisca un *bias* di per sé sufficientemente negativo. Cfr. WILDE, *IBorder Automates Discrimination,* in *www.iborderctrl.no/blog:iborderctrl_automates_discrimination*, consultato il 20/10/2021.

[49] Il legame tra l'intelligenza artificiale e la profezia che si autoavvera in sociologia è stata sviluppata da Merton e prende le mosse dal noto *Teorema di Thomas*, secondo cui situazioni definite come reali, lo diventano negli effetti. THOMAS, THOMAS, *The child in America: behavior problems and programs,* New York, 1928; MERTON, *La profezia che si autoavvera*, in *Teoria e Struttura Sociale*, II, Bologna, 1971.

[50] Così sostiene a proposito delle misure di prevenzione nostrane, MOCCIA, *Le misure*, cit., 3. L'autore sostiene che sia «*possibile, allora, parlare di fattispecie indiziarie di sospetto che fungono da sostitutivi di vere e proprie fattispecie criminose, risultate inapplicabili per carenza di necessari riscontri: una vera e propria truffa di etichette, del tipo di quelle che la giurisprudenza di Strasburgo rimerebbe a 'smascherare' tramite l'estensione della 'materia penale' e delle relative garanzie, sulla base di criteri di ordine sostanziale*».

elementi di fatto idonei a fondare la prognosi di pericolosità. Sotto questo profilo, sarebbe corretto escludere una presunzione in tal senso, considerando che tali condotte potrebbero derivare non necessariamente dalla volontà di ingannare il sistema, quanto da una sensazione di disagio rispetto al fatto di essere interrogati da un dispositivo di intelligenza artificiale.

Non di minor conto è il contrasto con il principio di difesa. Dovrebbe trovare applicazione l'obbligo di motivazione del provvedimento di diniego e il viaggiatore respinto dovrebbe avere il diritto a ottenere una spiegazione rispetto alla decisione adottata, affinché possa predisporre un'adeguata difesa in caso di impugnazione. A parte i costi legati al ricorso amministrativo, vi è una difficoltà oggettiva a spiegare quale sia stato il percorso a fondamento della decisione algoritmica[51].

Altri profili di criticità si pongono rispetto all'impiego di questo sistema. Sino a ora esso è stato testato in via sperimentale e su base volontaria, ma allorquando dovesse essere annoverato tra i legittimi e ordinari strumenti di controllo alle frontiere esterne, si potrebbero porre problemi relativi alle conseguenze nei casi in cui il viaggiatore si rifiuti di fornire i propri dati personali e biometrici. Gli sarà impedito il transito? Sarà automaticamente considerato un soggetto ad alto rischio? La condotta potrebbe integrare gli estremi di una fattispecie penale alla stessa stregua del *rifiuto di indicazioni sulla propria identità personale* prevista nel nostro ordinamento dall'art. 651 c.p.?[52].

L'evidenza dei contrasti che il ricorso a queste tecniche di controllo e prevenzione possono determinare rispetto ad alcuni principi fondamentali è tale da trovarne traccia in tutti i documenti europei dedicati alla regolamentazione delle nuove tecnologie[53].

---

[51] Prescindendo dal fatto che, per come è impostato il procedimento di autoapprendimento dell'intelligenza artificiale, non è possibile ricostruirne il percorso argomentativo, dovrebbe almeno essere prevista la possibilità di conoscere le categorie di dati che vengono di volta in volta utilizzate. Sul punto, si veda, CROCKETT-O'SHEA-SZEKEL-MALAMOU-BOULTADAKIS-ZOLTAN, *Do Europe's borders need multi-faceted biometric protection?*, in *Biometric Technology Today*, 2017, 7, 5-8.

[52] Si potrebbero configurare anche ipotesi come quelle previste rispettivamente dall'art. 4 *Testo Unico sulle leggi di pubblica sicurezza* (T.U.L.P.S.) e art. 294 del relativo regolamento rispetto all'ipotesi di mancata esibizione di un documento di identità.

[53] Sui rischi di discriminazione e conseguente violazione del principio di uguaglianza, ad esempio, il Regolamento UE 679/2016 prevede al *Considerando* n. 71 che siano «*impediti gli effetti discriminatori nei confronti delle persone fisiche base della razza o dell'origine etnica, delle opinioni politiche, della*

I nuovi strumenti si pongono anche in tensione con i principi di equità e proporzionalità, che sfuggono a una praticabilità algoritmica richiedendo un'attività interpretativa che solo l'uomo può garantire[54].
Analogamente a quanto affermato dalla Commissione di esperti in merito alle misure contenute nel pacchetto *Frontiere Intelligenti* e al sistema *Entry/Exit*, anche in relazione al *IBorderCtr* il complesso meccanismo creato sembra da ritenersi sproporzionato rispetto agli scopi di gestione delle frontiere e l'obiettivo appare comunque non raggiunto[55].

6. *Diritti fondamentali,* data mining *e possibili criticità.* I controlli alle frontiere sono sempre stati un fattore di alto rischio per possibili violazioni del divieto di discriminazione nonché per il pericolo di verificazione di episodi di umiliazione, degradazione o anche ostracismo rispetto sia a singoli individui sia a gruppi, né può sottovalutarsi il pericolo di quelli che sono stati definiti dei veri e propri *miscarriages of justice*[56].
Con l'implementazione del nuovo strumento, tali criticità potrebbero ridursi ove l'intelligenza artificiale venisse addestrata a trattare con le persone tenendo in considerazione le loro peculiarità e non l'appartenenza a gruppi cd. vulnerabili. Tuttavia, potrebbero sorgere anche ulteriori complicazioni e di-

religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti». Il dettato è di ampia portata e va riferito non solo alle attività di profilazione dei dati personale, quanto piuttosto a tutte le attività anche di tipo predittivo come il riconoscimento facciale. Cfr. SIMONCINI, *L'algoritmo*, cit., 84. Anche la Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti stilato dalla Cepej nell'ambito del Consiglio d'Europa ne dà conto al secondo principio, prevedendo il divieto «*di creare o accentuare discriminazioni tra gruppi e individui*». Cfr. QUATTROCOLO, *Intelligenza*, cit., *5*.

[54] Così SIGNORATO, *Giustizia penale*, cit., 611.

[55] Il Gruppo di Lavoro istituito in virtù dell'articolo 29 della Direttiva 95/46/CE aveva ritenuto che *il valore aggiunto di un sistema di ingressi/uscite ai fini del conseguimento di tali obiettivi non è un elemento sufficiente per dimostrarne la necessità e la proporzionalità in termini di ricadute sui diritti fondamentali, in particolare il diritto alla protezione dei dati e alla vita privata. Le ingerenze nella vita privata devono essere "necessarie in una società democratica" e il mero valore aggiunto non soddisfa il criterio di necessità in tale contesto.* Cfr. *www.ec.europa.eu/justice/policies/privacy/index_en.htm*

[56] Così ROBINS, *Former regulator warns of miscarriages of justice as a result of poor quality CCTV facial comparisons*, in www.thejusticegap.com, 2022. Sul punto v. anche DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.,* 2022, 3, 1057 ss. che ricorda l'episodio della finale della UEFA *Champions League* di Cardiff del 2017, durante la quale più di duemila persone furono identificate quali criminali da strumenti di riconoscimento facciale, 1066.

scriminazioni connesse ai possibili *bias* derivanti dalla qualità dei dati immessi dal programmatore nella fase di avvio del *machine learning*[57]. Infatti potrebbe realizzarsi una discriminazione algoritmica perché lo strumento di riconoscimento facciale offre la possibilità di classificare le persone, ad esempio, a seconda dell'etnia di appartenenza. Così in Cina, è in corso di sperimentazione un *software* di riconoscimento facciale che invia un segnale di pericolosità nel caso in cui il soggetto faccia parte della popolazione degli Uiguri[58]. In altro ambito, può ricordarsi il programma *COMPAS*, che, in uso nel Wisconsin, configurava, sulla base di dati acquisiti, un più elevato rischio di recidiva per gli imputati di colore[59].

Si potrebbe porre, persino, un problema di '*pregiudizi di ritorno*', nell'ipotesi in cui i *bias* che hanno influenzato l'intelligenza artificiale si riflettano anche sulla stessa guardia di frontiera che potrebbe appiattire il proprio giudizio sulle risultanze algoritmiche.

Un altro aspetto delicato, complesso da provare e valutare, è costituito dalle difficoltà di interazione tra essere umano e intelligenza artificiale. Soprattutto sul piano emotivo potrebbero generarsi forti equivoci (per esempio, come giudicherà la macchina un pianto, un errore, o una forte emozione?). Lo scenario è del tutto nuovo ed è facile immaginare che le persone potrebbero provare disagio a relazionarsi con un *avatar*, che, pur espressione di una tecnologia avanzata, non è certamente in grado di comprendere i bisogni emotivi umani[60]. Magari, in un prossimo futuro questo problema sarà superato, ove il

---

[57] ZICCARDI, *Sorveglianza elettronica, data mining e trattamento discriminatorio delle informazioni dei cittadini tra esigenze di sicurezza e diritti di libertà*, in *Ragion pratica*, 2018, 1, 28 ss. V., ampiamente, DELLA TORRE, *Tecnologie di riconoscimento facciale*, cit., 1066, ss.

[58] Cfr. *www.agendadigitale.eu/sicurezza/privacy/sorveglianza-di-massa-in-cina-cosi-funziona-il-modello-che-spaventa-loccidente/*. Si veda, altresì, *www.gendershades.org/overview.html*, che mette in correlazione i rischi di discriminazione per le minoranze etniche rispetto agli errori prodotti dai sistemi di riconoscimento facciale. Invero, il 4 aprile 2021 un tribunale cinese ha riconosciuto il diritto dei cittadini alla cancellazione dei propri dati acquisiti con le tecniche biometriche di rilevamento facciale, ponendo così un freno all'abuso di questi sistemi. In *www.wired.it/attualita/tech/2021/04/14/cina-riconoscimento-facciale-causa/*. Allo stesso modo, anche le discriminazioni di genere trovano l'avallo nell'uso di queste nuove tecnologie; sul punto si veda *www.gendershades.org/*.

[59] Si v. il caso *Supreme Court of Wisconsin, State of Wisconsin v. Eric L. Loomis, Case no. 2015AP157-CR, 5 April – 13 July 2016* con nota di CARRER, *Se l'amicus curiae è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin*, in *Giur. pen.* 2019, 4.

[60] Cfr. CROCKETT-O'SHEA-SZEKEL-MALAMOU-BOULTADAKIS-ZOLTAN, *Do Europe's borders need multi-faceted biometric protection?* cit., 5-8. Gli autori ipotizzano alcuni casi di incomprensione tra

rapporto uomo-macchina dovesse diventare la regola, ma nel frattempo la questione è rilevante[61].

I dati possono assumere una dimensione attiva – qualora costituiscano uno strumento di tutela dei diritti fondamentali o ne determinino una violazione - oppure una dimensione passiva, laddove rappresentino l'oggetto della tutela per essere stati impiegati in maniera illegittima, fraudolenta o senza il consenso del titolare.

Rispetto alla prima ipotesi, nell'impiego di *IBorderCtrl* i dati sono le due facce di una stessa medaglia. Da un lato, essi favoriscono un miglioramento nell'efficienza dei controlli alle frontiere esterne facilitando l'ingresso di coloro che ne hanno il diritto e garantendo la sicurezza di tutti[62]. Dall'altro invece, l'autorizzazione all'ingresso nell'area Schengen viene fatta dipendere in via esclusiva dalla raccolta dei dati dei viaggiatori e questo potrebbe tradursi in una violazione dei diritti di libertà.

Diversamente, in relazione alla misura passiva dei dati, non sembrerebbe porsi né un problema di *privacy*, né di titolarità del trattamento dei dati personali e biometrici[63], perché, nel caso dell'impiego di *IBorderCtrl,* il soggetto accede volontariamente alla piattaforma e ha conoscenza sin da subito delle finalità di impiego, esprimendo un consenso in fase di registrazione[64]. Resta il fatto però che la sottoposizione a questa forma di controllo è comunque precondizione per l'ingresso – con tutte le ricadute che questo comporta anche

---

l'uomo e la macchina: come potrebbe comportarsi la macchina in caso di reazioni emotive come il pianto del viaggiatore? E se la persona fornisce delle informazioni sbagliate per un mero errore materiale e le ritratta o fraintende la domanda, come verrà valutata questa circostanza dall'*avatar*? Sarà considerata una menzogna e contribuirà a innalzare l'indice di rischio della pericolosità sociale? Ulteriori questioni, poi, possono sorgere in tema di neuro- diversità, riferibile ai casi di autismo, depressione, traumi, dolore cronico, schizofrenia. Sul punto si veda WILDE, *IBorder*, cit., *passim.*

[61] Cfr. IENCA-ANDORNO, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life Sci Soc Policy*, 2017, 13, 5.

[62] Nel Codice Schengen al *Considerando n. 7* si afferma che le verifiche e i controlli frontalieri *dovrebbero* essere effettuati nel pieno rispetto della dignità umana; l'uso del verbo al condizionale lascia intendere che le difficoltà di gestione siano note e che, dunque, il rispetto delle garanzie non venga sempre garantito. Proprio il ricorso alle nuove tecnologie potrebbe contribuire a un miglioramento di tali condizioni.

[63] Per una definizione dettagliata di dato biometrico, si veda SACCHETTO, *Face to face: il complesso rapporto tra automated facial recognition thecnology e processo penale*, in *www.lalegislazionepenale.it*, 18 ottobre 2020, 2. Si veda, altresì, la citata Proposta di Regolamento del 21 aprile 2021, 21, 45.

[64] Certo potrebbero non mancare rischi di scarsa informazione e comprensione rispetto al trattamento dei dati. Cfr. *www.iborderctrl.eu/The-project.*

sul consenso.

Al momento, l'unico quadro normativo di riferimento è offerto dalla *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* del 1981 (modificata dal protocollo del 2018) e che, a differenza del GDPR, comprende anche i dati trattati per motivi di sicurezza nazionale e difesa. I dati raccolti durante l'intervista dall'*avatar* rientrano, con ogni probabilità, nella categoria dei dati considerati dalla Convenzione oggetto di tutela e, pertanto, per essi opera il consenso prestato dal viaggiatore. Semmai la questione riguarda attività di *profiling* che l'algoritmo promuove anche raccogliendo dati contenuti in archivi non istituzionali presenti nel *web*. Per questa categoria di dati dovrebbe trovare applicazione la disciplina contenuta nel D.lgs. del 18 maggio 2018 n. 51[65] che all'art. 3 stabilisce che i dati siano raccolti per finalità determinate, esplicite e legittime e trattati in modo lecito, corretto, adeguato, pertinente e non eccessivo rispetto alle finalità per le quali sono utilizzati. È, inoltre, vietata (art. 8) la profilazione, a meno che non vengano applicate garanzie adeguate per i diritti e le libertà dell'interessato[66]. In ogni caso deve essere garantito il diritto di ottenere l'intervento umano.

Le ipotesi di conservazione o trasferimento a soggetti terzi dei dati così raccolti sono già oggetto di specifiche disposizioni nella regolamentazione degli altri sistemi di ingresso in uso in Europa, che prevedono la conservazione dei dati in archivi per un limitato periodo di tempo e consentono la loro cessione soltanto in ipotesi tassative. Queste soluzioni dovrebbero, ragionevolmente, essere adottate anche nel caso in cui *IBorderCtrl* divenga operativo in maniera definitiva[67].

I dati posti alla base del funzionamento di *IBorderCtrl* non sono solo quelli forniti dal viaggiatore, ma anche i *data set* che sono utilizzati per alimentare l'apprendimento automatico del sistema di intelligenza artificiale. Garantire la

[65] Decreto di attuazione della direttiva (UE) 2016/680 del Parlamento e del Consiglio, del 27 aprile 2016, relativa *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 e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[66] Si tratta della trasposizione degli artt. 4 e 11 della Direttiva.

[67] Nell'attuale fase sperimentale è previsto che le informazioni raccolte siano cancellate dal sistema immediatamente dopo l'effettuazione del controllo.

qualità e la trasparenza di questa tipologia di dati significa garantire la sicurezza del sistema; purtuttavia, si tratta di condizioni che difficilmente possono essere assicurate[68]. Il principio di trasparenza tecnica, sancito da documenti come la Carta etica del Cepej e la Proposta di Regolamento del 21/04/2021[69], è infatti impossibile da rispettare, dal momento che neanche i programmatori riescono a mantenere il controllo su tutto il procedimento[70].

La mancanza di trasparenza e accessibilità dei dati potrebbe comportare la lesione del diritto di difesa, qualora il visitatore a cui è stato negato l'attraversamento dei confini europei decida di impugnare il provvedimento di diniego[71].

Il tema dell'accuratezza dei dati acquisisce un'importanza ancora maggiore ove si consideri che essi costituiscono il fondamento anche degli stessi sistemi di riconoscimento facciale. Sarebbe allora necessario incidere sulla qualità dei dati iniziali utilizzati per l'addestramento dell'intelligenza artificiale, chiamati a soddisfare stringenti criteri di qualità secondo quanto previsto anche dall'art. 10 della Proposta di Regolamento.

7. *Qualche osservazione in tema di riconoscimento facciale*. Dai documenti europei più recenti sulle nuove tecnologie si evince che le criticità rilevate sono maggiori dei vantaggi. Si esprime, ad esempio, in questo senso il Comitato consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale[72], secondo cui gli strumen-

[68] In tema di equità algoritmica e trasparenza, si veda BARABAS, *Beyond Bias: "Ethical AI" in Criminal Law*, in *The Oxford Handbook of Ethics of AI*, 2020, 1-21.

[69] Il mito della trasparenza e neutralità è ancora largamente diffuso: l'art. 13 della Proposta di Regolamento del 21 aprile 2021 è rubricato *Trasparenza e fornitura di informazioni agli utenti.* Per la Carte etica del Cepej, si veda *www.rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348*. Persino il Consiglio di Stato del nostro paese ha invocato un *principio di trasparenza rafforzato* come fondamento degli algoritmi. Così Cons. St., Sez. IV, 8 aprile 2019, n. 2270.

[70] La neutralità degli algoritmi è condizionata sia dalla qualità dei dati sia dalle correlazioni operate dagli stessi sistemi. Cfr. SIGNORATO, *Giustizia penale*, cit., 611 ss. Si è anche sostenuto che l'algoritmo è autore di valutazioni predittive conservatrici, nella misura in cui analizza dati che appartengono al passato per prevedere un comportamento futuro. Sul punto cfr. PASQUALE, *The black box society: the secret algorithms that control money and information*, Harward, 2016.

[71] Cfr. ENGSTROM et al., *Government by algorithm: artificial intelligence in Federal Administrative Agencies,* in *www.acus.gov/sites/default/files/documents/Government%20by%20Algorithm.pdf, 2020, 10/2020.*

[72] Si tratta della cd. *Convenzione 108+* del Consiglio d'Europa del 28 gennaio1981, modificata da un

ti preposti al riconoscimento facciale possono entrare in conflitto con valori quali la dignità umana, il principio di non discriminazione e la libertà di espressione[73]. Il Comitato europeo per la protezione dei dati ha pubblicato il 29 gennaio 2020 le Linee guida sul trattamento dei dati attraverso dispositivi video, secondo cui le tecniche di riconoscimento facciale sono consentite solo se rispettano i principi di liceità, necessità, proporzionalità e minimizzazione dei dati, così come previsto anche dal GDPR del 2016. Si richiede inoltre che il loro impiego sia preceduto da valutazioni di impatto sui diritti e sulle libertà fondamentali[74]. Sul punto lo stesso Comitato si è pronunciato nuovamente il 21 giugno 2021[75] ribadendo, in un parere congiunto con il Garante europeo per la protezione dei dati personali a commento della Proposta di regolamentazione dell'intelligenza artificiale, i timori suscitati dall'impiego di tecniche di identificazione biometrica a distanza delle persone in spazi pubblicamente accessibili. Nel documento si suggerisce di vietare l'uso di dispositivi per riconoscere automaticamente volti, andatura, impronte digitali, DNA, voce e altri segnali biometrici o comportamentali, in qualsiasi contesto. Si raccomanda, altresì, di *vietare i sistemi di intelligenza artificiale che utilizzano la biometria per classificare gli individui in gruppi basati su etnia, genere, orientamento politico o sessuale, o altri motivi per i quali la discriminazione è vietata ai sensi dell'articolo 21 della Carta dei diritti fondamentali*. Le tecniche di riconoscimento facciale emozionale sono considerate *altamente indesiderabili* e si ritiene debbano *essere vietate, ad eccezione di casi molto specifici, come alcuni scopi sanitari*.

I timori si amplificano ulteriormente quando si analizza la tecnologia alla base di *IBorderCtrl*. L'aspetto più controverso riguarda proprio il sistema di riconoscimento *affettivo*, che non si limita ai dati biometrici, ma analizza le emozioni delle persone tramite l'analisi dei micro-gesti facciali non verbali. L'intelligenza artificiale cd. *emozionale* riesce a cogliere i livelli di stress e ansia, esaminando i biomarcatori di inganno e permettendo, così, di distinguere

protocollo del 2018.

[73] L'affermazione è contenuta nelle *Linee-guida in materia di intelligenza artificiale e protezione dei dati* del 25 gennaio 2019. Si veda *www.rm.coe.int/guidelines-on-facial-recognition/1680a134f3*.

[74] Cfr. *www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf*

[75] Si veda *www.edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_it.pdf*.

i viaggiatori in buona fede da quelli non in buona fede. Questo procedimento pone a rischio un principio primario come quello del rispetto della dignità umana[76].

Nelle Linee Guida 05/2022 sull'uso della tecnologia del riconoscimento facciale da parte delle forze dell'ordine, il Comitato ha ribadito che l'identificazione biometrica a distanza di persone in spazi accessibili al pubblico comporta un elevato rischio di intrusione nella vita privata degli individui e non trova posto in una società democratica in quanto per natura comporta una sorveglianza di massa. Di qui la riaffermazione dell'indesiderabilità dell'uso del riconoscimento facciale o di tecnologie simili per dedurre le emozioni di una persona fisica e della necessità di prevedere un divieto esplicito[77]. Su posizioni analoghe si collocava già il Parlamento europeo in una sua Risoluzione del 2021.

Seppure impiegato in Inghilterra e negli Stati Uniti[78], il riconoscimento facciale ha suscitato molte critiche e destato perplessità[79], sia per il suo fondamento scientifico, sia per i problemi di proporzione rispetto alle finalità di prevenzione del crimine. In riferimento a quest'ultimo punto, infatti, si profilerebbe una violazione del principio di autodeterminazione della persona e una possibile lesione della libertà morale[80], non giustificabile neanche con le esigenze di ordine pubblico e sicurezza della collettività[81]. Invero, nella specifica ipotesi di *IBorderCtrl* la questione potrebbe subire un ridimensionamento, ove si verificassero alcune condizioni.

La prima consiste nel garantire il principio di trasparenza e conoscibilità algo-

---

[76] In tema cfr. DELLA TORRE, *Tecnologie di riconoscimento facciale*, cit., 1071 ss.

[77] *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 1.0* Adopted on 12 May 2022, § 104, *www.edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf*.

[78] In Inghilterra il sistema è stato impiegato nel 2011 proprio per il controllo alle frontiere dal *Border Agency*. Cfr. MONEDERO-DENCIK, *The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl,* in *Information, Communication and Society*, 2020, 8, 1.

[79] Così BOFFEY, *EU border 'lie detector' system criticised as pseudoscience,* in *www.theguardian.com/world/2018/nov/02/eu-border-lie-detection-system-criticised-as-pseudoscience*, 11/2018; si veda anche *https://www.agendadigitale.eu/sicurezza/privacy/sorveglianza-di-massa-in-cina-cosi-funziona-il-modello-che-spaventa-loccidente/*, 3/2020. Si veda anche *www.iborderctrl.no/*.

[80] Sul punto KOSTORIS, *Genetica, neuroscienze e diritto penale*, in *Genetics, Robotics, Law, Punishment*, a cura di Provolo-Riondato-Yenisey, Padova, 2014, 344.

[81] Cfr. *Artificial intelligence and robotics for law enforcement*, UNICRI-Interpol, Torino, 2019, 13.

ritmica già indicato genericamente per i dati e per il quale la Proposta di Regolamento del 21 aprile 2021 prevede un preciso obbligo in caso di sistemi di rilevamento biometrico[82].

Un'altra condizione riguarda il necessario consenso di chi accede al servizio e la possibilità di mantenerne il controllo. Tuttavia, rispetto al requisito del consenso in alcuni Paesi[83], taluni nodi non sembrano ancora essere sciolti, al punto che viene vietato l'utilizzo indiscriminato delle tecniche di riconoscimento facciale nei luoghi pubblici, non potendo le persone in transito prestare di volta in volta il consenso. Come accennato, nel caso di *IBorderCtrl*, il consenso è prestato all'atto della registrazione sulla piattaforma dedicata e, pertanto, il rispetto dell'autodeterminazione del singolo sembrerebbe assicurato, almeno formalmente[84].Tuttavia, le Linee guida sul riconoscimento facciale del Consiglio d'Europa del 2021 fanno rilevare come il consenso da solo non sia sufficiente a giustificare l'utilizzo del riconoscimento facciale da parte della pubblica autorità, giacché tra questa e i soggetti privati ci sarà sempre uno squilibrio di poteri[85]. La consapevolezza dei soggetti coinvolti non garantisce, infatti, la cd. libertà cognitiva[86] e il rischio di un *effetto Panopticon* è sempre in agguato, con il pericolo di una lesione del diritto alla riservatezza nel senso più ampio del termine[87].

---

[82] Così il Titolo IV alla pagina 73 della citata Proposta, recante *obblighi di trasparenza per determinati sistemi di AI.*

[83] In USA, il *Biometric Information Privacy Act dell'Illinois*, il *Washington's Biometric identifiers Act* e Il *Personal Identify Information Act* del Texas, ritengono il consenso elemento fondante delle tecniche di riconoscimento facciale. Cfr. GIRASA, *Artificial Intelligence as a disruptive technology. Economic Transformation and Government Regulation*, Svizzera, 2020, 1 ss.

[84] Sul punto si veda CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Dir. pen. uomo*, 2021, 5, 12.

[85] V. *Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Convention 108, Guidelines on Facial Recognition Directorate General of Human Rights and Rule of Law, in www.rm.coe.int/guidelines-on-facial-recognition/1680a134f3*, 6.

[86] La libertà cognitiva è considerata un'estensione del diritto alla libertà di manifestazione del pensiero ed è un concetto di recente acquisizione che non ha ancora trovato un esplicito riconoscimento giuridico. Cfr. SOMMAGGIO-MAZZOCCA-GEROLA-FERRO, *Cognitive liberty. A first step towards a human neuro-rights declaration*, in *BioLaw J.*, 2017, 3, 27, *passim*. Si veda anche DI GIOVINE, *Ripensare il diritto penale attraverso le (neuro) scienze?*, Torino, 2020.

[87] Cfr. RODOTÀ, *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, in *www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293*. Simili attività di profilazione e riconoscimento facciale potrebbero dare luogo a un rischio di giudizio del soggetto fuori contesto rispetto alla situazione in cui erano stati raccolti i dati oggetto di valutazione algoritmica.

Sarebbe opportuno, inoltre, capire cosa prevedrà la disciplina normativa eventualmente adottata al termine della sperimentazione di *IBorderCtrl* rispetto all'ipotesi in cui il viaggiatore neghi il suo consenso: se sarà prevista una soluzione alternativa ovvero sarà negato l'accesso all'area Schengen.
Quanto alla garanzia del pieno rispetto del principio di autodeterminazione, essa può essere assicurata solo se – oltre alla conoscibilità e al consenso espresso – l'utente possa mantenere sempre il dominio sulle sue scelte, indipendentemente dalla complessità del sistema che sta utilizzando, così come è previsto anche dal quinto principio della Carta Etica del Cepej[88]. Le nuove tecnologie, infatti, devono costituire un'opportunità e un vantaggio e per la collettività e per il singolo - e non un limite vincolante a carattere negativo.
I timori, in tema di riconoscimento facciale, permangono. La Proposta di Regolamento del 21 aprile 2021 compie una doppia valutazione di impatto e di rischio.
Da un lato, al *Considerando* n. 39 si richiedono cautele ulteriori nell'impiego dei sistemi di intelligenza artificiali in materia di migrazione, asilo e controlli alle frontiere, potendo questi avere effetti su persone che si trovano spesso in una posizione particolarmente vulnerabile. Dall'altro, sono previste significative restrizioni all'uso dei sistemi di rilevamento biometrico, perché considerati ad alto rischio e consentiti solo per attività di *law enforcement* alle forze dell'ordine.
Segnatamente, i sistemi di rilevamento biometrico remoto in tempo reale sono – in linea di principio – consentiti solo in tre ipotesi specifiche: per la ricerca mirata di potenziali vittime specifiche di reato; per la prevenzione di una minaccia imminente alla vita o all'incolumità, anche in caso di attacco terroristico; per l'individuazione e l'identificazione degli autori di reati gravi. Si tratta di una casistica, tassativa, che include anche le finalità di contrasto sottese a *IBorderCtrl*, ossia il contrasto alla criminalità transfrontaliera[89].

---

[88] *Il quinto principio è relativo al "controllo da parte dell'utilizzatore",* ed è così formulato: *"precludere un approccio prescrittivo e assicurare che gli utilizzatori siano attori informati e abbiano il controllo delle loro scelte".* Sul punto QUATTROCOLO, *Intelligenza*, cit., 9.
[89] La Proposta al *Considerando* n. 23 chiarisce, altresì, che la disciplina ha valore di *lex specialis* rispetto alle maglie più larghe previste dall'art. 10 della Direttiva (UE) 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*

Il problema del riconoscimento facciale è stato esaminato solo in rari casi dalla giurisprudenza. La Corte EDU, muovendosi nella prospettiva della necessità e della proporzionalità della misura, in alcune recenti pronunce ha sottolineato che il diritto alla protezione della propria immagine presuppone il diritto dell'individuo di controllarne l'uso e che l'art. 8 della convenzione debba ritenersi violato qualora la polizia conservi le immagini di un soggetto a tempo indeterminato, senza che la normativa interna preveda sufficienti garanzie[90]. Dal canto loro, le decisioni delle Corti nazionali sono poco numerose, oltre che di segno contrastante.

Una prima sentenza, destinata a costituire un *leading case*, è quella emessa dall'*High Court of Justice* di Cardiff. Oggetto del procedimento era il sistema di riconoscimento facciale in uso in via sperimentale al corpo di polizia del Galles e ritenuto dal ricorrente lesivo del diritto alla riservatezza *ex* art. 8 Cedu, contrario alla Direttiva (UE) 2016/680 rispetto alla tutela del trattamento dei dati personali, nonché violativo dell'*Equality Act* del 2010 relativo al contrasto alle forme di discriminazione[91]. Contrariamente alle aspettative, i giudici inglesi hanno respinto i motivi di doglianza del ricorrente e ritenuto il sistema di rilevamento biometrico conforme alla disciplina vigente. Quanto alla possibile violazione della Cedu, la Corte ha ritenuto che l'ingerenza nella vita privata del singolo fosse giustificata ai sensi dell'art. 8 par. 2 Cedu, ricorrendone le condizioni di legalità e di necessità. In particolare, i giudici hanno sottolineato la sussistenza della proporzione tra lo scopo di prevenzione dei reati e il sacrificio dei diritti del singolo, rilevando, inoltre, che non sarebbe stata rag-

---

perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. Il dettato del citato art. 10 prevede che *il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orien-tamento sessuale è autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: a) se autorizzato dal diritto dell'Unione o dello Stato membro; b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato.*

[90] Corte EDU 11 giugno 2020, *P.N. c. Germania,* § 56: Corte EDU 13 febbraio 2020, *Gaughran c. Regno Unito*, § 96.

[91] Per un esame approfondito del funzionamento del sistema e della decisione della Corte si veda DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice,* in *Dir. pen. cont.*, 2020, 1, 231-247.

giunta la prova circa la possibile influenza sul sistema di pregiudizi razziali o di genere. La Corte ha, quindi, ritenuto lecito e trasparente il trattamento dei dati, poiché, in mancanza di corrispondenza tra le immagini catturate dal sistema e i nominativi inseriti negli elenchi in possesso delle forze dell'ordine, i dati raccolti sono cancellati immediatamente.

La giurisprudenza italiana non ha affrontato diffusamente lo specifico tema del riconoscimento facciale[92], ma appare significativa una pronuncia relativa alla possibilità di introdurre nel processo penale delle prove fondate sulle nuove tecnologie. Nel caso di specie, si tratta di una richiesta di revisione di una sentenza di condanna per un fatto di violenza sessuale su minore, in cui il ricorrente chiede che sia valutata la prova della sua innocenza raggiunta tramite l'utilizzo dei metodi *IAT* e *aIAT*. Tali strumenti sarebbero in grado – ad avviso di chi li ha ideati – di provare la verità dei ricordi impliciti di una persona, tramite la valutazione strumentale del contenuto della memoria del condannato, tenuto conto dei tempi di reazione rispetto ad affermazioni che descrivono fatti autobiografici[93]. I nuovi strumenti sono stati ritenuti dalla Corte di Appello di Brescia[94] contrari al dettato degli artt. 64 co. 2 e 188 c.p.p., in quanto capaci di influenzare la libertà di determinazione o di alterare la capacità di ricordare e valutare i fatti, circostanza che non può essere ritenuta lecita nemmeno in presenza del consenso dell'interessato, non essendo la libertà morale un diritto disponibile o rinunciabile in alcun modo. La compressione della capacità di autodeterminazione, infatti, costituisce un limite invalicabile per l'attività probatoria, tanto più che il consenso sarebbe viziato *ab origine*, non potendo il soggetto conoscere prima il contenuto della sua memoria im-

[92] Su come invece la tecnologia relativamente al riconoscimento facciale stia entrando nello strumentario a disposizione delle forze dell'ordine in Italia, al di fuori dell'intervento del legislatore; sull'atteggiamento di sostanziale "disinteresse" della Cassazione in ordine al problema; sulla moratoria nei confronti dell'installazione di in luoghi pubblici o aperti al pubblico di impianti di videosorveglianza con riconoscimento facciale e le relative eccezioni (d.l. 8 ottobre 2021 n. 139, convertito con modifiche dalla l. 3 dicembre 2021, n. 205) v., ampiamente, DELLA TORRE, *Le tecnologie di riconoscimento facciale*, anche per la bibliografia citata, cit., 1075 ss.

[93] V. PAGLIANO, *L'algoritmo e le neuroscienze: la chimera per smascherare le menzogne?*, in *Diritto penale e intelligenza artificiale. Nuovi scenari*, a cura di Balbi-De Simone-Esposito-Manacorda, Torino 2022, 91 ss.

[94] Corte App. Brescia, Sez. II, sentenza 11 novembre 2020 n. 1683, in *file:///C:/Users/fdsde/OneDrive/Desktop/giorgia/sent%20brescia/1607551213_sentenza-corte-appello-brescia-test-iat.pdf*.

plicita.
Mutuando il ragionamento della giurisprudenza di merito e applicando le sue risultanze anche al di fuori della sede processuale, si dovrebbe arrivare a escludere le nuove tecnologie utilizzate per prendere delle decisioni che incidono sui diritti di libertà dell'individuo, qualora il soggetto stesso non sia posto nella condizione di mantenere il controllo e l'autodeterminazione della sua persona. È, appunto, il caso di *IBorderCtrl*, nel momento in cui l'*avatar* analizza le microespressioni facciali del viaggiatore e questi, pur prestando il consenso, non è in grado di conoscere anticipatamente i movimenti del viso che saranno oggetto di valutazione.

8. *Rilievi conclusivi.* Nel bilanciamento degli interessi coinvolti dal sistema *IBorderCtrl* tutto sembra prendere le mosse dal connubio tra la *società del rischio* e la *società della sicurezza*[95], tanto da giustificare il sacrificio di alcuni beni giuridici, ancorché fondamentali, promuovendo forme di sorveglianza di massa dagli esiti incerti e rischiosi[96]. Rispondono pienamente a questo schema strumenti di anticipazione della tutela *praeter delictum* come le misure di prevenzione, con cui *IBorderCtrl*[97] presenta talune analogie. Più in generale, molte linee di politica europea sembrano orientate in tale direzione, vista anche l'entità di investimenti che l'Unione europea ha disposto per l'incremento di strumenti a tutela della sicurezza[98].
I rischi sono tuttavia fortemente avvertiti dalla collettività: prova ne siano le forti polemiche suscitate in Francia dall'approvazione della legge sulla '*Sicurezza globale*' del 15 aprile 2021, che permette alle forze di polizia di tutelare l'ordine pubblico facendo liberamente uso della capillare rete di videosorveglianza cittadina, di droni e sistemi di sorveglianza intelligente come *bo-*

[95] Cfr. FOCAULT, *Sicurezza, popolazione e territorio, Corso al Collège de France* 1977-1978, Milano, 2005, 15 ss.
[96] Il pericolo di un rapporto direttamente proporzionale tra avanzamento delle istanze di sicurezza e regressione dei diritti fondamentali e delle tutele è denunciato da molti. Sul punto si veda CELOTTO, *I 'non diritti' al tempo di internet,* in *Dir. Internet*, 2019, 2, 238 e DE MINICO, *Costituzione, emergenza e terrorismo*, Napoli, 2016, 95 ss.
[97] Sull'anticipazione del rischio nelle società moderne, si veda PELISSERO, *Le misure*, cit., 4-5.
[98] Il mercato europeo della sicurezza muove un giro di affari enorme e in costante crescita. Sul punto si veda l'interessante *report* contenuto in *www.altreconomia.it/europa-sicurezza/*.

dycam[99].

È pur vero che in tempi di forti migrazioni, rischi terroristici e finanche pericoli pandemici, non è più immaginabile che il controllo alle frontiere sia affidato solo al riscontro facciale effettuato da un agente rispetto a una immagine apposta su un passaporto o al suo istinto: in questa luce *IBorderCtrl* potrebbe costituire non solo un rischio, ma anche un'opportunità. Le ricadute positive di questo strumento sull'efficacia in concreto dei controlli alle frontiere sono evidenti e si misurano in termini di velocità delle operazioni, uniformità nei controlli, scoperta delle false identità.

Tutto ciò a patto, però, che gli *standard* di verifica siano molto elevati, i risultati affidabili, i controlli continui e rigorosi[100], perché la valutazione del rischio criminale e il *profiling* non necessariamente si traducono in attività violative dei diritti fondamentali. È piuttosto il rischio di valutazioni discriminatorie a contenere *in nuce* un pericolo di violazione dei diritti[101], nonché di esclusione sociale sulla base di un generico rischio criminale[102].

Tuttavia, l'era della quarta rivoluzione[103] ci impone di non adottare posizioni di sfiducia algoritmica che portino a vietare *a priori* l'impiego dei nuovi strumenti, né a considerare i diritti delle persone in contrapposizione al progresso tecnologico come in un rapporto inversamente proporzionale. Piuttosto dovrebbe trovare ampia applicazione il principio di precauzione[104], nel conti-

---

[99] La *Legge di Sicurezza globale* è stata presentata in Parlamento il 20 ottobre 2020 e ha suscitato forti proteste nella popolazione, sfociate in numerose manifestazioni di piazza. Il generale rafforzamento dei poteri riconosciuti alle forze dell'ordine, in aggiunta al dettato dell'art. 24 che prevede l'incarcerazione e una multa elevata per coloro – giornalisti compresi – che diffondono immagini relative al volto a ad altro elemento identificativo (al di fuori del numero di identificazione individuale) di agenti di reparti operativi, ha incontrato anche il parere sfavorevole dell'ONU che ha inviato al Presidente francese una Raccomandazione in merito. Cfr. *www.penshare.it/cose-la-legge-sicurezza-globale-francese/*.

[100] SIGNORATO, *Giustizia penale*, cit., 616.

[101] Sul punto Commissione LIBE del Parlamento europeo, in *www.eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017DC0261&from=EN*, secondo cui i rischi di lesione dei diritti fondamentali aumentano quando i sistemi informatici sono interoperabili, rendendo accessibili contemporaneamente dati sensibili come razza, etnia, salute, genere, credo religioso, etc. Alcuni hanno anche sostenuto che i sistemi come *IBorderCtrl* finiscano per automatizzare la discriminazione; sul punto si veda WILDE, *IBorder*, cit., *passim*.

[102] Sui rischi di esclusione sociale dei soggetti considerati pericolosi, si veda CAVALIERE, *Punire*, cit., 97 ss.

[103] Così FLORIDI, *La quarta rivoluzione. Come l'infosfera sta rivoluzionando il mondo*, Milano, 2017, *passim*.

[104] Più ampiamente sul punto SIMONCINI, *L'algoritmo*, cit., 86 ss., secondo cui si impone una tutela

nuo sforzo di bilanciamento tra progresso tecnologico e tutele, allorquando si versi in una condizione di *incertezza conoscitiva*[105].

Potrebbe aiutare nell'intento anche una efficace regolamentazione rispetto alle ipotesi di responsabilità dei danni causati dalla scarsa qualità dei dati o dal loro errato trattamento, che non rimanga a livello di mera enunciazione di principio, come nel caso dell'art. 25 GDPR[106]. Più in generale, è necessaria e non più rinviabile l'adozione di una normativa di dettaglio vincolante che regolamenti tutte le tipologie di strumenti e tutti i loro possibili usi[107].

La previsione che l'uomo non affidi la verifica in via esclusiva ai nuovi strumenti e mantenga sempre un controllo sui risultati[108], la possibilità di impugnativa del provvedimento e anche la previsione di un Garante[109] sono misure che contribuiscono ad aumentare le tutele rispetto all'impiego dell'intelligenza artificiale.

Determinante, inoltre, potrebbe essere l'individuazione di parametri di validazione dei sistemi, sulla falsariga di quanto previsto nel 1993 dalla Corte Suprema degli Stati Uniti con i *Daubert standard* e che ha trovato l'avallo anche della Corte di Cassazione italiana nel 2010[110].

---

preventiva dei diritti fondamentali già in fase di progettazione dei nuovi sistemi (sia nel momento *by design*, sia *by default*). Si veda anche GAMBINI, *Algoritmi e sicurezza,* in *Giur. it.*, 2019, 7, 1726 ss. Sul principio di precauzione in diritto penale si veda, tra gli altri, PIERGALLINI, *Danno da prodotto e responsabilità penale: profili dommatici e politico-criminali*, Milano, 2004; CASTRONUOVO, *Principio di precauzione e diritto penale. Paradigmi dell'incertezza nella struttura del reato*, Aprilia, 2012; CONSORTE, *Tutela penale e principio di precauzione. Profili attuali, problematicità, possibili sviluppi*, Torino, 2013, CORN, *Il principio di precauzione nel diritto penale. Studio sui limiti all'anticipazione della tutela penale*, Torino, 2013; DEL TUFO, *Principio di precauzione e gestione del rischio: quali spazi applicativi per il diritto penale?* in *La prova scientifica nel processo penale*, a cura di Carlizzi-Tuzet, Torino, 137 ss.

[105] Si veda SIMONCINI, *Diritto costituzionale e decisioni algoritmiche*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di Dorigo, Pisa, 61.

[106] GDPR - Regolamento generale sulla protezione dei dati (UE/2016/679) Articolo 25 *Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita.*

[107] Cfr. CURRAO, *Il riconoscimento*, cit., 23.

[108] La citata Proposta di Regolamento del 21 aprile 2021 dedica l'intero art. 14 al tema della sorveglianza umana rispetto alla progettazione e all'impiego delle nuove tecnologie. Il *Considerando* n. 65, poi, prevede che i sistemi considerati ad alto rischio siano valutati e certificati da soggetti terzi, estranei alla fase di progettazione. GIRASA, *Artificial Intelligence*, cit., 1 ss.

[109] Così è previsto anche per le attività di *Frontex*, per le quali è istituito un responsabile dei diritti fondamentali. Cfr. *www.frontex.europa.eu/it/cosa-facciamo/diritti-fondamentali/*.

[110] Cass., Sez. IV, 17 dicembre 2010, n. 43786. Si veda MAUGERI, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali*, in *Arch. pen.*, 2021, 1, 1-37.

Queste le misure di tutela, ma molto dipenderà dalla capacità di combinare la conoscenza causale con la conoscenza scientifica e la conoscenza statistica, riconoscendo un ruolo preminente all'etica[111]. Dei ventitré *Principi di Asilomar*[112]*,* ben tredici sono dedicati all'etica e ai valori che devono ispirare l'intelligenza artificiale, tra cui l'allineamento dei valori di tali sistemi ai valori umani durante il loro funzionamento e la necessità che la loro progettazione e gestione sia compatibile con la dignità umana, i diritti, la libertà e la diversità culturale.

Anche l'Unesco, nelle recentissime Raccomandazioni adottate in tema di utilizzo dell'intelligenza artificiale[113], sottolinea l'importanza di adottare dei principi '*propulsori*' dell'etica condivisi globalmente. Il documento esplicita a livello internazionale, per la prima volta, l'importante principio secondo cui i sistemi di intelligenza artificiale non possono essere impiegati per scopi di sorveglianza di massa e aggiunge, inoltre, che, quando si adottano norme preordinate a utilizzare tali strumenti di controllo, gli Stati membri devono garantire che la responsabilità ultima sia sempre di un essere umano. Il documento è stato sottoscritto da 193 Paesi, tra i quali anche la Cina, invitata così a porre volontariamente dei limiti all'utilizzo di strumenti di sorveglianza di massa.

L'Unione europea sembra, invece, avere due visioni diverse. Da un lato, infatti, la Commissione autorizza la sperimentazione di un sistema come *IBorderCtrl* in nome della sicurezza sovranazionale, che rischia di tradursi proprio in strumenti di sorveglianza di massa, dall'altro anticipa la linea adottata dall'Unesco, mostrando un atteggiamento di estrema cautela nei documenti più volte citati in questo contributo. Infine, sembra tornare sui suoi passi quando il 6 ottobre 2021 il Parlamento europeo adotta una Risoluzione su

[111] Si veda POWERS-GANASCIA, *Ethics of ethics of AI,* in *The Oxford Handbook of Ethics of AI,* a cura di Dubber-Pasquale-Das, Oxford, 2020, 1 ss.

[112] I *Principi di Asilomar* sono stati stilati nel 2017 e sottoscritti dagli scienziati più autorevoli tra cui anche Stephen Hawking. Si tratta di un testo suddiviso in tre aree: la prima sulla *ricerca*, la seconda su *etica e valori*, la terza e ultima sui *problemi di scenario*.

[113] Il documento è particolarmente importante perché si tratta del primo accordo internazionale in tema di etica dell'intelligenza artificiale, Raccomandazione sull'etica dell'intelligenza artificiale, adottata il 23 novembre 2021, cfr., in particolare, 3.2, par. 36 e 37

intelligenza artificiale e diritto penale[114], in cui si esprime profonda preoccupazione proprio per i progetti di ricerca finanziati nell'ambito di *Horizon 2020* che diffondono l'intelligenza artificiale alle frontiere esterne, come il progetto *IBorderCtrl*. Nel documento si invita la Commissione a introdurre il divieto di trattamento dei dati biometrici, comprese le immagini facciali in grado di determinare sorveglianza di massa negli spazi accessibili al pubblico, e a interrompere il finanziamento di ricerca o diffusione della biometrica o di programmi che potrebbero portare alla sorveglianza di massa.

Sembra, allora, che ancora una volta ci si trovi di fronte al *dilemma di Collingridge*[115] e che, anche per strumenti così nuovi e complessi come quello appena utilizzato ai confini Schengen, si dovrà decidere se regolare la tecnologia quando è ancora giovane e poco conosciuta, cercando di anticipare le possibili conseguenze inaspettate o indesiderate, o attendere che tali conseguenze si palesino, con il rischio di perdere il controllo sulla loro regolamentazione.

Resta fermo che neppure *IBorderCtrl* potrà aiutare a comprendere se un viaggiatore, pur mentendo, sia effettivamente in procinto di compiere un reato, perché «*nonostante le fascinazioni della fisica quantistica, il comportamento umano non è prevedibile, essendo l'uomo un essere libero, sempre capace di autodeterminazione al netto dei condizionamenti esterni*»[116].

[114] Il testo è rinvenibile in *www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.pdf*.

[115] Il *dilemma di Collingridge* è un dilemma metodologico in cui gli sforzi per influenzare o controllare l'ulteriore sviluppo della tecnologia affrontano due livelli di problemi. Il primo è un problema di informazione: gli impatti non possono essere previsti facilmente fino a quando la tecnologia non sarà ampiamente sviluppata e ampiamente utilizzata. Il secondo è un problema di potere: il controllo o il cambiamento sono difficili quando la tecnologia si è radicata. Il dilemma è un punto di riferimento fondamentale nei dibattiti sulla valutazione della tecnologia. Cfr. COLLINGRIDGE, *The Social Control of Technology*, Londra, 1980, *passim*.

[116] POWERS-GANASCIA, *Ethics*, cit., 64.