

AI ACT*, pratiche vietate e controlli alle frontiere esterne dell'Unione europea

Francesca Di Gianni

SOMMARIO: 1. Introduzione. – 2. I sistemi di intelligenza artificiale al servizio della *Fortress Europe*. – 3. Il regolamento (UE) 2024/1689: alcuni chiarimenti preliminari. – 3.1. *Segue: predictive policing* e rischi di discriminazione alle frontiere esterne dell'Unione europea. – 3.2. *Segue: art. 5, par. 1, lett. f)* e divieto dei sistemi di riconoscimento delle emozioni: *an obvious loophole* nel settore dei controlli alle frontiere? – 3.3. *Segue: esenzione dei sistemi di categorizzazione biometrica* utilizzati nelle attività di contrasto e rischi di violazione del diritto alla protezione dei dati personali dei migranti per esigenze di sicurezza. – 4. Conclusioni.

1. *Introduzione.*

I sistemi di intelligenza artificiale (IA) sembrano contenere la promessa di una semplificazione di una serie indefinita di operazioni nei settori più diversificati, grazie alla capacità di raccolta e di analisi di grandi quantità di dati, impiegati per una migliore valutazione dei rischi, il miglioramento di previsioni e la realizzazione di attività molto più rapidamente di quanto sarebbe possibile per l'uomo¹. Questa promessa sembra valere anche per la gestione delle frontiere, rispetto alle quali l'IA appare dotata di un immenso potenziale per rivoluzionare il sistema di *governance* delle migrazioni², semplificando e velocizzando i controlli d'identità e l'analisi dei dati su visti e richiedenti protezione internazionale³.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a *double-blind peer review*.

¹ H. Tyler, *The Increasing Use of Artificial Intelligence in Border Zones Prompts Privacy Questions*, in *Migration Information Source*, www.migrationpolicy.org, 2 February 2022.

² A. Beduschi, *International Migration Management in the Age of Artificial Intelligence*, in *Migration Studies*, 2021, p. 576-596.

³ L. Everuss, *AI, Smart Borders and Migration*, in A. Elliott (eds.), *The Routledge Social Science Handbook of AI*, London, 2021, p. 339-356.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

Il ricorso all'IA in questo contesto ha registrato un significativo aumento soprattutto per effetto della pandemia da SARS-Cov-2⁴, la quale ha prodotto un processo di ridefinizione dei confini e un rafforzamento dei controlli⁵ attraverso l'integrazione di funzionalità di *artificial intelligence* per la creazione di c.d. *smart borders*⁶.

Ai continui tentativi di erigere e rafforzare le frontiere fisiche (come muri e barriere) si è gradualmente affiancata una progressiva estensione delle *virtual frontiers*⁷, basate sull'implementazione di tecnologie per l'identificazione, la profilazione e l'analisi dei rischi⁸, rendendo l'IA uno strumento chiave nell'ambito dell'intero ciclo migratorio⁹. Questi sistemi sono già da tempo una realtà in Paesi come il Canada, in cui strumenti decisionali algoritmici vengono utilizzati nel processo di gestione delle domande di asilo dal 2014¹⁰, ma anche al confine tra Stati Uniti e Messico dove gli algoritmi vengono utilizzati per stabilire l'eventuale necessità di porre un migrante irregolare in detenzione preventiva¹¹, mentre nel 2020, il Ministro degli interni del Regno Unito ha deciso di eliminare il c.d. *streaming*

⁴ A. Beduschi, M. McAuliffe, *Artificial Intelligence, Migration and Mobility: Implications for Policy and Practice*, in M. McAuliffe – A. Triandafyllidou (eds.), *World Migration Report 2022*, Geneva, 2022, p. 1.

⁵ F. L. Collins, *Geographies of Migration III: The Digital Migrant*, in *Progress in Human Geography*, 2023, p. 738-749.

⁶ P. Trauttmansdorff, *Borders, Migration, and Technology in the Age of Security: Intervening with STS*, in *Italian Journal of Science and Technology Studies*, 2022, p. 133-154.

⁷ In generale, sul tema della costruzione di barriere e muri per il controllo delle frontiere si veda A. Ruiz Benedicto – M. Akkerman – P. Brunet, *A Walled World Towards a Global Apartheid*, Centre Délas d'estudios par la pau, Barcelona, November 2020. Sull'applicazione del «controllo a distanza» nei controlli alle frontiere si veda A. R. Zolberg, *Managing a World on the Move*, in *Population and Development Review*, 2006, p. 222-253; F. Delioglu, *Technology at the Borders: Surveillance, Control and Resistance in Eu Migration Governance*, in *Balsillie Papers*, www.balsilliepapers.ca, 2025.

⁸ European Parliament, *Artificial Intelligence at EU Borders. Overview of Applications and Key Issues*, European Parliamentary Research Service, p. 1, www.europar.europa.eu, July 2021.

⁹ F. Delioglu, *op. cit.*

¹⁰ P. Molnar – L. Gill, *Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System*, in *International Human Rights Program*, Toronto, www.citizenlab.ca, 2018.

¹¹ R. Koulisch, *Immigration Detention in the Risk Classification Assessment Era*, in *Connecticut Public Interest Law Journal*, 2017, p. 1-35.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

algorithm in uso dal 2015 per elaborare le domande di visto poiché considerato causa di un *hostile environment* per i richiedenti¹².

Questa tendenza ha inevitabilmente travolto anche l'Unione europea (UE) che, nell'ambito del processo di costruzione di «uno spazio di libertà, sicurezza e giustizia senza frontiere interne in cui sia assicurata la libera circolazione delle persone» – che richiede, come noto, l'adozione e l'applicazione di «misure appropriate per quanto concerne i controlli alle frontiere esterne, l'asilo, l'immigrazione [...]» ai sensi dell'art. 3, par. 2, del Trattato sull'Unione europea (TUE) – si è affidata sempre più ai sistemi di intelligenza artificiale in questo settore¹³.

Il ricorso a questi strumenti ha segnato una profonda trasformazione dell'architettura del sistema dell'Unione europea dei controlli alle frontiere che si è sostanzialmente attestata sulla dicotomia (eccessivamente semplificata) di «sicurezza vs. mobilità», determinando una modifica delle pratiche tradizionali in favore di una dinamica di securitizzazione¹⁴ e di un approccio di *governance* delle frontiere decentralizzato e digitalizzato quale risposta ai rischi percepiti per la sicurezza causati dai crescenti flussi migratori verso l'UE. La creazione delle *virtual frontiers* costituisce infatti una delle principali componenti del processo di esternalizzazione dei controlli alle frontiere¹⁵, quale strumento volto a ridurre la pressione migratoria sugli

¹² H. McDonald, *Home Office to Scrap «Racist Algorithm» for UK Visa Applicants*, in *The Guardian*, www.theguardian.com, 4 August 2020; C. Barclay – E. Guild, *Brexit, Personal Data and Aliens*, in *Immigration, Asylum and Nationality Law*, 2023, p. 271 ss.; N. Vavoula, *Tr-AI-Nsforming Migration, Asylum and Border Management in the EU: The Roles of the Ai Act, Interoperable Large-Scale it Systems and EU Migration Agencies*, www.papers.ssrn.com, March 2024.

¹³ Sul punto si veda S. Penasa, *Artificial Intelligence and the Governance of Migration: Potentialities and Pitfalls between Technological Neutrality and Political Design*, in *Opinio Juris in Comparatione*, 2022, pp. 97-115.

¹⁴ Così J. De Coninck, G. Raimondo, *Understanding European Border Management. A Tale of Transformation and Orchestrated Impunity*, in *Verfassungblog on Matters Constitutional*, www.verfassungblog.de, 27 February 2024.

¹⁵ Con l'espressione «esternalizzazione» ci si riferisce allo spostamento di responsabilità nell'attuazione dei controlli e nel monitoraggio dei confini verso Paesi terzi di origine e di transito dei migranti, nonché ad alcune attività svolte dall'Unione e dagli Stati membri sul territorio di tali Paesi. A partire dal 2015, il crescente afflusso di migranti ha dato inizio ad un processo per l'implementazione di strumenti digitali e il rafforzamento dei controlli nei principali Paesi di origine e di transito. Ciò si è tradotto in un rinnovato interesse a fornire e supportare l'uso di tecnologie di sorveglianza nei Paesi terzi, con l'obiettivo finale di prevenire le partenze e tali tecnologie, sebbene ritenute necessarie per

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

Stati membri dell'UE «di primo ingresso» e, al contempo, mezzo per evitare che i migranti intraprendano viaggi pericolosi per raggiungere il territorio dell'Unione¹⁶.

Questo modello di politica migratoria basato sui tre pilastri della securizzazione, dell'esternalizzazione e della digitalizzazione delle frontiere esterne dell'Unione europea ha trovato la sua consacrazione, *in primis*, nel Nuovo Patto sulla migrazione e l'asilo¹⁷ e nei relativi atti legislativi adottati il 22 maggio 2024¹⁸ che nel delineare il nuovo approccio dell'UE alla

prevenire la criminalità e il terrorismo, si rivelano estremamente intrusive e di ostacolo al godimento dei diritti fondamentali per le popolazioni locali e per le persone in movimento. Si veda sul tema P. Trauttmansdorff, *Borders, Migration, and Technology in the Age of Security: Intervening with STS*, in *Italian Journal of Science and Technology Studies*, 2022, p. 133-154; Euromed Rights, *Artificial Intelligence: The New Frontier of the EU's Border Externalisation Strategy*, www.euromedrights.org, July 2023; A. Tagliapietra, *Technologies and Borders. The EU is Digitalizing Migration Externalization*, in *GMF*, www.gmfus.org, 2 October 2023; P. De Pasquale, *L'esternalizzazione dei controlli di frontiera e dei diritti dei migranti dell'Unione europea e degli Stati membri del Mediterraneo*, in *Studi sull'integrazione europea*, 2024, p. 183-197; E. Xanthopoulou, *Mapping EU Externalization Devices through a Critical Eye*, in *European Journal of Migration and Law*, 2024, p. 108-135;

¹⁶ Sul tema dell'esternalizzazione si rinvia, segnatamente, a V. Moreno-Lax, *Assessing Asylum in Europe: Extraterritorial Border Controls and Refugee Rights under EU Law*, Oxford, 2017; V. Papageorgiou, *The Externalization of European Borders*, 2018, www.kedisa.gr; A. Del Valle-Gálvez, *Refugee Crisis and Migrations at the Gates of Europe: Deterritoriality, Extraterritoriality and Externalization of Border Controls*, in *Journal of International Law and International Relations*, 2019, p. 117-160; D. Vitiello, *Le frontiere esterne dell'Unione europea*, Bari, 2020; I. Goldner Lang, *External Border Control Techniques in the EU as a Challenge to the Principle of Non-Refoulement*, in *European Constitutional Law Review*, 2021, p. 1-29; J. De Conick, G. Raimondo, *op. cit.*

¹⁷ Comunicazione della Commissione, del 23 settembre 2020, Un nuovo patto sulla migrazione e l'asilo, COM(2020) 609 final.

¹⁸ Il pacchetto approvato comprende dieci atti, vale a dire la direttiva (UE) 2024/1346 del Parlamento europeo e del Consiglio, del 14 maggio 2024, recante norme relative all'accoglienza dei richiedenti protezione internazionale; il regolamento (UE) 2024/1347 del Parlamento europeo e del Consiglio, del 14 maggio 2024, recante norme sull'attribuzione a cittadini di paesi terzi o apolidi della qualifica di beneficiario di protezione internazionale, su uno status uniforme per i rifugiati o per le persone aventi titolo a beneficiare della protezione sussidiaria e sul contenuto della protezione riconosciuta, che modifica la direttiva 2003/109/CE del Consiglio e che abroga la direttiva 2011/95/UE del Parlamento europeo e del Consiglio; il regolamento (UE) 2024/1348 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che stabilisce una procedura comune di protezione internazionale dell'Unione e abroga la direttiva 2013/32/UE; il regolamento (UE) 2024/1349 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che stabilisce una procedura di rimpatrio alla frontiera e che modifica il regolamento (UE)

questione migratoria, riforma l'intero sistema di gestione delle migrazioni prevedendo, *inter alia*, un rafforzamento della sorveglianza digitale¹⁹.

Questo rafforzamento appare supportato ulteriormente dal neonato regolamento (UE) 2024/1689, del 13 giugno 2024, sull'intelligenza artificiale (d'ora in poi *AI Act*)²⁰ che, con l'intento di istituire «un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione»²¹, interviene anche in relazione all'implementazione dei sistemi di IA nella gestione delle migrazioni e delle

2021/1148; il regolamento (UE) 2024/1350 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che istituisce un quadro dell'Unione per il reinsediamento e l'ammissione umanitaria e modifica il regolamento (UE) 2021/1147; il regolamento (UE) 2024/1351 del Parlamento europeo e del Consiglio, del 14 maggio 2024, sulla gestione dell'asilo e della migrazione, che modifica i regolamenti (UE) 2021/1147 e (UE) 2021/1060 e che abroga il regolamento (UE) n. 604/2013; il regolamento (UE) 2024/1352 del Parlamento europeo e del Consiglio, del 14 maggio 2024, recante modifica dei regolamenti (UE) 2019/816 e (UE) 2019/818, allo scopo di introdurre accertamenti nei confronti dei cittadini di paesi terzi alle frontiere esterne; il regolamento (UE) 2024/1356 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che introduce accertamenti nei confronti dei cittadini di paesi terzi alle frontiere esterne e modifica i regolamenti (CE) n. 767/2008, (UE) 2017/2226, (UE) 2018/1240 e (UE) 2019/817; il regolamento (UE) 2024/1358 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che istituisce l'«Eurodac» per il confronto dei dati biometrici ai fini dell'applicazione efficace dei regolamenti (UE) 2024/1351 e (UE) 2024/1350 o del Parlamento europeo e del Consiglio e della direttiva 2001/55/CE del Consiglio e ai fini dell'identificazione dei cittadini di paesi terzi e apolidi il cui soggiorno è irregolare, e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, che modifica i regolamenti (UE) 2018/1240 e (UE) 2019/818 del Parlamento europeo e del Consiglio e che abroga il regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio.

¹⁹ Sul tema del rafforzamento dell'impiego delle tecnologie digitali in materia migratoria determinato dal Nuovo Patto si veda, *inter alia*, S. Marinai, *Il rafforzamento del controllo digitale nel Nuovo Patto sulla migrazione e l'asilo*, in *I Post di AISDUE*, Focus «La proposta di Patto su immigrazione e asilo», 2020, p. 119-140; ID., *La riforma del sistema di informazione visti: tra esigenze di sicurezza dello spazio Schengen e istanze di tutela dei richiedenti asilo*, in *Diritto, Immigrazione e Cittadinanza*, 2022, p. 66-91. Inoltre, in senso critico, si veda L. Salgado – H. Beirens, *What Role Could Digital Technologies Play in the New EU Pact on Migration and Asylum?*, Migration Policy Institute, www.reliefweb.int, December 2023; PICUM, *The EU Migration Pact: A Dangerous Regime of Migrant Surveillance*, www.picum.org, 11 April 2024.

²⁰ Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 202/1828 (regolamento sull'intelligenza artificiale).

²¹ Considerando 1.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

frontiere, sollevando non poche perplessità per i rischi potenziali di una grave compromissione della tutela dei diritti dei migranti che potrebbero derivarne²².

Sebbene il regolamento sull'intelligenza artificiale riconosca il ruolo primario della protezione dei diritti in questione, anche delle persone migranti, da una lettura critica del suo testo emerge un risultato diverso, fatto di eccezioni e salvaguardie attenuate dei diritti umani anche con riferimento a quelle pratiche per le quali è stabilito dall'art. 5 un divieto di immissione, messa in servizio ed utilizzo in quanto considerate «inaccettabili» proprio per i possibili effetti che producono sui diritti.

Fatte tali premesse, il presente contributo intende proporre un'analisi critica delle pratiche vietate *ex art. 5 dell'AI Act* che rilevano nel contesto considerato e individuare le principali lacune e le problematiche derivanti dal regime di eccezioni e salvaguardie limitate dei diritti fondamentali delle persone migranti cui la norma dà vita a causa della mancata esclusione dal campo di applicazione del divieto di determinati sistemi di IA cui si fa sempre più ricorso (o a cui l'UE prevede di ricorrere) nell'ambito della *governance* della migrazione e, in specie, dei controlli alle frontiere esterne.

2. I sistemi di intelligenza artificiale al servizio della Fortress Europe.

Al fine di contenere la crescente pressione migratoria e, quindi, di filtrare e prevenire l'attraversamento delle frontiere da parte di migranti considerati indesiderati²³, l'Unione europea ha gradualmente sperimentato e introdotto sistemi di valutazione del rischio, poligrafi automatici e tecnologie di sorveglianza per il controllo degli arrivi²⁴, segnando un

²² Sul punto, B. Frelick – I.M. Kysel – J. Podkul, *The Impact of Externalization of Migration Controls on the Rights of Asylum Seekers and other Migrants*, in *Journal on Migration and Human Security*, 2016, p. 190-220; S.F. Nicolosi, *Externalisation of Migration Controls: A Taxonomy of Practices and Their Implications in International and European Law*, in *Netherlands International Law Review*, 2024, p. 1-20; M.C. Carta, *La dimensione esterna della politica migratoria dell'Unione europea. Nuovo Patto: sempre più verso gli accordi e i «non-accordi» di esternalizzazione dei controlli e delle responsabilità*, *Rivista Quaderni AISDUE*, 2024, p. 1-39.

²³ F. Delioglu, *op. cit.*

²⁴ Sul punto, si veda European Commission, *Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security*, www.op.europa.eu, May 2020; FRONTEX, *Artificial Intelligence-Based Capabilities for the European Border and Coast Guard*, Final Report, Warsaw, www.frontex.europa.eu, 17 March 2021; European Parliament,

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

cambiamento nella logica di gestione delle sue frontiere verso il c.d. *tecnosolutionism*²⁵ che ha determinato una vera e propria «*digitalisation of the European migration policy*»²⁶ e ha aggiunto un ulteriore tassello al processo di costruzione della Fortezza Europa²⁷.

In linea generale, la creazione delle frontiere intelligenti²⁸ è stata incentrata, *in primis*, sullo sviluppo e l'interconnessione di sistemi informativi centralizzati su larga scala e, dunque, sulla elaborazione di strumenti come i

Artificial Intelligence at EU Borders, cit.; A.M. Eklund, *Rule of Law Challenges of «Algorithmic Discretion» and Automation at EU Border Control. A Case Study of ETLAS Through the Lens of Legality*, in *European Journal of Migration and Law*, 2023, p. 249-274.

²⁵ N. Vavoula, *op. cit.*

²⁶ M. Besters – F.W.A. Brom, «*Greedy*» *Information Technology: The Digitalization of the European Migration Policy*, in *European Journal of Migration and Law*, 2010, p. 455-470.

²⁷ G. Campesi, *Policing Mobility Regimes. Frontex and the Production of the European Borderscape*, London, 2023, p. 13-35; Statewatch, *Automating the Fortress: Digital Technologies and European Borders*, www.statewatch.org, 6 June 2024. L'uso delle tecnologie più innovative è ormai saldamente radicato nella politica migratoria europea, il che trova conferma, da ultimo, nella *European Integrated Border Management strategy* presentata dalla Commissione europea a marzo del 2023. Questa strategia definisce «*la visione comune europea per la gestione integrata delle frontiere europee nei prossimi cinque anni*» (2023-2027) e chiarisce il ruolo chiave che la tecnologia dovrebbe svolgere all'interno di tale nuova visione. In particolare, l'«*European integrated border management, especially border checks and border surveillance, should be supported by advanced, mobile and interoperable European technical systems and solutions that are compatible with large-scale EU IT systems. This is to guarantee more efficient and reliable border controls*», con l'obiettivo di garantire mezzi e metodi uniformi di controllo delle frontiere in tutta l'UE, così da «*prevenire e contrastare l'immigrazione irregolare, migliorare l'efficacia dei rimpatri, prevenire la criminalità transfrontaliera e facilitare i viaggi legittimi*», Comunicazione della Commissione, del 14 marzo 2023, che definisce la politica strategica pluriennale per la gestione europea integrata delle frontiere, COM(2023) 146 final, p. 3-8.

²⁸ La Commissione europea ha avviato nel 2011 il processo di costruzione delle *smart borders* per migliorare la sicurezza delle frontiere nell'Unione europea (UE) facendo ricorso alle nuove tecnologie. Si veda, la Comunicazione della Commissione, del 25 ottobre 2011, *Frontiere intelligenti – Opzioni e prospettive*, COM(2011) 680 definitivo. Inoltre, in dottrina si veda P. Lehtonen – P. Aalto, *Smart and Secure Borders through Automated Border Control Systems in EU? The Views of Political Stakeholders in the Member States*, in *European Security*, 2017, p. 207-225; P.J. Pesch – F. Boehm, *Smart Border is Watching You! Fundamental Rights Implications of Automated Data Processing and Decision-making at the EU Border*, in *Law Research Paper Series*, 2023, p. 1-39.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

sistemi di informazione Schengen (SIS)²⁹, di informazione visti (VIS)³⁰ e Eurodac³¹, originariamente concepiti per operare in modo indipendente e

²⁹ Il sistema d'informazione Schengen (SIS), creato nel 1995, è una banca dati che opera a sostegno del controllo delle frontiere esterne e della cooperazione nelle attività di contrasto tra gli Stati membri dell'[Accordo di Schengen](#) (attualmente, 25 [Stati membri](#) dell'UE e quattro Paesi associati). Nel 2006, l'originario sistema SIS è stato sostituito e rafforzato dal sistema SIS II, operativo dal 2013, a norma dei regolamenti (CE) n. 1986/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'accesso al sistema di informazione Schengen di seconda generazione (SIS II) dei servizi competenti negli Stati membri per il rilascio delle carte di circolazione e (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen di seconda generazione (SIS II). Alla luce delle sfide in materia migratoria, anche il SIS II è stato ulteriormente rafforzato dai regolamenti (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema di informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare; (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'Accordo di Schengen e abroga il regolamento (CE) n. 1987/2006; e (UE) 2018/1826 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione.

³⁰ Istituito dal regolamento (CE) n. 676/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata, più volte sottoposto a modifica tra cui, da ultimo, dal regolamento (UE) 2023/2667 del Parlamento europeo e del Consiglio, del 22 novembre 2023, che modifica i regolamenti (CE) n. 767/2008, (CE) n. 810/2009 e (UE) 2017/2226 del Parlamento europeo e del Consiglio, i regolamenti (CE) n. 693/2003 e (CE) n. 694/2003 del Consiglio e la Convenzione di Applicazione di Schengen, per quanto riguarda la digitalizzazione della procedura di visto.

³¹ Istituito con regolamento (CE) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino, poi modificato dal regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (rifusione), che a partire dal 12 giugno 2026

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

poi resi progressivamente interoperabili³², nonché l'Entry/Exit System (EES)³³, il sistema europeo di informazione ed autorizzazione ai viaggi (ETIAS)³⁴ e il sistema centralizzato per individuare gli Stati membri in

verrà abrogato e sostituito dal regolamento (UE) 2024/1358 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che istituisce l'«Eurodac» per il confronto dei dati biometrici ai fini dell'applicazione efficace dei regolamenti (UE) 2024/1351 e (UE) 2024/1350 del Parlamento europeo e del Consiglio e della direttiva 2001/55/CE del Consiglio e ai fini dell'identificazione dei cittadini di paesi terzi e apolidi il cui soggiorno è irregolare, e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, che modifica i regolamenti (UE) 2018/1240 e (UE) 2019/818 del Parlamento europeo e del Consiglio e che abroga il regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio.

³² L'Unione europea ha sviluppato un quadro per l'interoperabilità tra i suoi sistemi IT su larga scala nei settori delle frontiere, dei visti, della cooperazione di polizia e giudiziaria, dell'asilo e della migrazione basato sui regolamenti (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio e (UE) 2018/818, del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816.

³³ Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di Applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011.

³⁴ L'ETIAS è un sistema informatico automatizzato, sviluppato dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) che verrà introdotto entro la fine del 2026, per poi diventare obbligatorio nel 2027, che si occupa del rilevamento dei rischi per la sicurezza e di quelli legati alla migrazione irregolare o a epidemie determinati dai visitatori esenti da visto che viaggiano nello spazio Schengen, al contempo assicurando il rispetto dei loro diritti fondamentali. Il sistema è stato istituito dal regolamento (UE) del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

possesto di informazioni sulle condanne pronunciate a carico di cittadini di Paesi terzi e apolidi (ECRIS-TCN)³⁵ di recente elaborazione.

Accanto a questi strumenti, nell'ultimo decennio sono stati elaborati sia da parte dell'UE che dei suoi Stati membri sistemi di intelligenza artificiale per supportare e migliorare l'efficienza della verifica dell'identità, del controllo e della sicurezza delle frontiere. Si pensi, per esempio, ai sistemi di rilevamento delle emozioni testati in Ungheria, Grecia e Lettonia³⁶ o all'uso del riconoscimento del dialetto nelle procedure di asilo in Germania³⁷, ma non solo. La maggior parte degli Stati membri dell'Unione dispone oggi di banche dati contenenti una quantità immensa di dati biometrici (come impronte digitali e profili di DNA) che possono essere consultati tramite avanzati algoritmi informatici³⁸.

Inoltre, il programma di finanziamenti della Commissione europea, Horizon 2020, ha poi messo a disposizione 1,3 miliardi di euro per la realizzazione di diversi progetti per il controllo dei confini, tra cui il progetto quadriennale ROBORDER, completato nell'agosto 2021³⁹; il progetto iBorderCtrl in Grecia, con cui sono state sviluppate tecnologie di riconoscimento facciale e di *lie detection*⁴⁰; il progetto TRESSPASS, che grazie all'utilizzo degli algoritmi, raccoglie ed elabora dati per l'identificazione del

³⁵ Il sistema ha la funzione di identificare gli Stati membri dell'UE che detengono informazioni sulle condanne pronunciate a carico di cittadini di Paesi terzi e apolidi che è stato creato dal regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziari, e che modifica il regolamento (UE) 2018/1726.

³⁶ European Commission, *Intelligent Portable Border Control System*, www.cordis.europa.eu, 3 September 2024.

³⁷ Per una panoramica dell'ampia gamma di nuove tecnologie, tra cui i sistemi di intelligenza artificiale, utilizzati alle frontiere, all'arrivo e dopo l'arrivo nell'UE si veda D. Okzul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*, www.rsc.ox.ac.uk, 2023.

³⁸ F. Ragazzi – E.M. Kuskonmaz – I.Z. Plájás – R. van de Ven – B. Wagner, *Biometric and Behavioural Mass Surveillance in EU Member States*, Report of the Greens/EFA in the European Parliament, www.scholarlypublications.universiteitleiden.nl, October 2021.

³⁹ Con una dotazione di circa 8 milioni di euro, l'obiettivo del progetto era sviluppare un sistema autonomo di sorveglianza delle frontiere basato sull'utilizzo di robot mobili senza pilota, dotati di telecamere ottiche, a infrarossi e termiche, nonché di sensori radar e a radiofrequenza per rilevare minacce ambientali e, soprattutto, migranti irregolari. Informazioni dettagliate sul progetto sono reperibili *online*: www.cordis.europa.eu.

⁴⁰ *Ibidem*.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

livello di rischio di ogni possibile ingresso all'interno dei confini statali⁴¹; il progetto pilota FOLDOUT per il rilevamento dei migranti irregolari attraverso il fogliame nelle regioni interne e più esterne dell'UE, ricorrendo ad un sistema che combina sensori e tecnologie in una piattaforma di rilevamento intelligente⁴².

E il ricorso all'IA si è esteso anche alle frontiere marittime. Nel 2019, l'Agenzia europea della guardia di frontiera e costiera (Frontex) ha commissionato uno studio a REND Europe, *think tank* specializzata in ricerca e sviluppo, per valutare l'eventuale implementazione di sistemi di IA nella gestione dei confini dell'UE. L'anno seguente ha sottoscritto un accordo con la Direzione generale per la migrazione e gli affari interni della Commissione europea (DG-HOME) per la supervisione e l'attuazione di progetti di ricerca relativi a questioni di sicurezza delle frontiere⁴³ e, nel 2021, ha rinnovato il contratto con la società israeliana Windward per l'utilizzo di una piattaforma di *maritime analytics*⁴⁴ che Frontex utilizza per contrastare e prevenire l'immigrazione irregolare, oltre alla criminalità transfrontaliera e al terrorismo.

Un ulteriore, significativo passo in questa direzione è stato compiuto con l'adozione del regolamento (UE) 2024/1689 sull'intelligenza artificiale che ha segnato senza dubbio «*a historic moment*»⁴⁵, trattandosi del primo tentativo organico di regolamentare l'impiego dei sistemi di intelligenza artificiale a livello mondiale, anche nel settore della gestione delle migrazioni e dei controlli alle frontiere esterne.

⁴¹ *Ibidem*.

⁴² *Ibidem*.

⁴³ DG-HOME, Frontex, *Terms of Reference between the Directorate-General for Migration and Home Affairs of the European Commission and the European Border and Coast Guard Agency Regarding the Role of the European Border and Coast Guard Agency in the Parts of the Framework Programme for Research and Innovation which Relate to Border security*, www.prd.frontex.europa.eu, 5 February 2020.

⁴⁴ Questa piattaforma utilizza sistemi di *reporting* marittimo, inclusi i dati di posizione provenienti dai transponder *Automatic Identification System* (AIS) delle navi, per controllare movimenti sospetti delle imbarcazioni. Il testo dell'accordo è reperibile *online*: www.ted.europa.eu.

⁴⁵ European Commission, *Statement by President von der Leyen on the Political Agreement on the EU AI Act*, www.ec.europa.eu, 9 December 2023.

3. *Il regolamento (UE) 2024/1689: alcuni chiarimenti preliminari.*

Componente fondamentale di un più ampio pacchetto di misure a sostegno dello sviluppo di un'IA affidabile – che comprende il pacchetto sull'innovazione in materia di IA⁴⁶, il lancio delle fabbriche di IA⁴⁷ e il piano coordinato sull'IA⁴⁸ – l'*AI Act* persegue due obiettivi paralleli e distinti, ma reciprocamente funzionali ovvero sia migliorare il funzionamento del mercato interno e promuovere l'adozione di un'IA antropocentrica e affidabile, nonché sostenere l'innovazione, al contempo garantendo «un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali [...] contro gli effetti nocivi dei sistemi di intelligenza artificiale (IA) nell'Unione» (art. 1, par. 1).

Come noto, per raggiungere i suddetti obiettivi il regolamento stabilisce una serie di regole armonizzate per l'immissione sul mercato e l'uso dei sistemi di IA nell'Unione, divieti di talune pratiche di IA, requisiti specifici per i sistemi considerati «ad alto rischio» e obblighi per gli operatori di tali sistemi (fornitori, *deployer*, importatori e distributori, fabbricanti), regole di trasparenza per determinati sistemi e regole armonizzate per l'immissione sul mercato di modelli di IA, nonché regole di monitoraggio e vigilanza del mercato e misure a sostegno dell'innovazione (art. 1, par. 2, lett. a-g))⁴⁹.

In particolare, ricorrendo ad un approccio *risk-based* volto ad adattare la tipologia e il contenuto delle norme del regolamento «all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA» (considerando 26), l'*AI Act* distingue i sistemi di IA in quattro categorie di

⁴⁶ Comunicazione della Commissione, del 24 gennaio 2024, sulla promozione delle start-up e dell'innovazione nell'intelligenza artificiale affidabile, COM(2024) 28 final. Inoltre, si veda European Commission, *Commission Launches AI Innovation Package to Support Artificial Intelligence Startups and SMEs*, www.ec.europa.eu, 24 January 2024.

⁴⁷ European Commission, *AI Continent Action Plan*, www.digital-strategy.ec.europa.eu, 9 April 2025.

⁴⁸ Comunicazione della Commissione, del 21 aprile 2021, Promuovere un approccio europeo all'intelligenza artificiale, COM(2021) 205 final.

⁴⁹ Il contenuto del regolamento richiederebbe ben altri approfondimenti. La dottrina sul tema è amplissima. Per una panoramica generale e dettagliata e per ulteriori riferimenti bibliografici si rinvia, *ex multis*, a F. Donati – G. Finocchiaro – F. Paolucci – O. Pollicino, *La disciplina dell'intelligenza artificiale*, Torino, 2025.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

rischio, dipendenti dalla gravità del danno che potrebbero determinare per la salute, la sicurezza o, appunto, i diritti fondamentali⁵⁰.

Per quanto ci interessa, è da evidenziare che il regolamento muove dalla consapevolezza che accanto ai molteplici utilizzi benefici, molti sono i rischi che l'IA possa essere utilizzata impropriamente e possa fornire strumenti nuovi «per pratiche di manipolazione, sfruttamento e controllo sociale [...] contrarie ai valori dell'Unione relativi al rispetto della dignità umana, alla libertà, all'uguaglianza, alla democrazia e allo Stato di diritto e ai diritti fondamentali sanciti dalla Carta, compresi il diritto alla non discriminazione, alla protezione dei dati e alla vita privata e i diritti dei minori» e che come tali andrebbero vietate (considerando 28).

Orbene, l'art. 5 individua quei sistemi di cui è vietata l'immissione sul mercato, la messa in servizio o uso nell'UE trattandosi di sistemi che pongono «rischi inaccettabili»⁵¹. Tuttavia, l'elenco delle pratiche vietate di

⁵⁰ In particolare, distingue: 1) sistemi che pongono «rischi inaccettabili», la cui immissione sul mercato, messa in servizio o uso sono vietati nell'UE (Capo II, art. 5, Pratiche di IA vietate); 2) sistemi c.d. «ad alto rischio», definiti in base ai requisiti di cui all'art. 6, par. 1, lett. a) e b) ed elencati nell'Allegato III al regolamento, per la cui immissione e utilizzo è richiesto il rispetto di stringenti requisiti e di una serie di obblighi da parte dei fornitori e degli altri soggetti interessati (Capo III); 3) sistemi che presentano «rischi di trasparenza» (Capo IV), rispetto ai quali i fornitori devono garantire che le persone fisiche siano informate del fatto di stare interagendo con un sistema di IA; e 4) sistemi a «rischio minimo», per i quali è prevista l'adozione di codici di condotta volti a promuovere l'applicazione volontaria anche a questi sistemi di AI dei requisiti previsti per i sistemi ad alto rischio (Capo X). L'applicazione del regolamento ha inizio a decorrere dal 2 agosto 2026. Tuttavia, in linea con quanto stabilito all'art. 113, il Capo I sulle «Disposizioni generali» e il Capo II relativo alle «Pratiche di IA vietate» sono diventati operativi già dal 2 febbraio 2025, mentre il Capo III, sezione 4, i Capi V, VII e XII e l'art. 78 si applicheranno a partire dal 2 agosto 2025, ad eccezione dell'art. 101 («Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali»), e le ultime disposizioni, vale a dire l'art. 6, par. 1, e i corrispondenti obblighi, che saranno applicabili dal 2 agosto 2027.

⁵¹ La norma include tra i sistemi di intelligenza artificiale la cui immissione sul mercato, messa in servizio o uso sono vietati quei sistemi che utilizzano tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli (par. 1, lett. a); che sfruttano le vulnerabilità di una persona fisica o di uno gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica (lett. b); per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note (lett. c) che possono dar vita ad un trattamento pregiudizievole o sfavorevole; per effettuare valutazioni del rischio al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei

cui all'art. 5, par. 1, presenta non poche problematiche, non solo perché alcuni sistemi di IA sono stati *wrongly classified*⁵² ma anche, e soprattutto, a causa del regime di eccezione previsto dalla norma in relazione all'applicazione del divieto con riferimento ad alcune delle pratiche contemplate nel contesto della migrazione e del controllo alle frontiere.

3.1 *Segue: predictive policing e rischi di discriminazione alle frontiere esterne dell'Unione europea.*

Innanzitutto, per quanto qui interessa, rileva il divieto di cui alla lett. d) del par. 1 dell'art. 5⁵³, il quale, oltre ad apparire vago e privo di chiarezza, prevede un'ampia deroga che potrebbe limitarne significativamente l'impatto. In particolare, la norma vieta i sistemi di IA che valutano o prevedono il rischio che una persona fisica commetta un reato basandosi esclusivamente sulla profilazione o sulla valutazione di tratti e caratteristiche della personalità, dove il termine «profilazione» indica, secondo quanto indicato dall'art. 3, par. 52, «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta

tratti e delle caratteristiche della personalità (lett. d); che creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso (lett. e); per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione (lett. f); di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale (lett. g); ed infine, sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto (lett. h).

⁵² N. Vavoula, *Regulating AI at EU's Borders. Where the AI Act Falls Short*, in *Verfassungsblog*, www.verfassungsblog.de, 13 December 2024.

⁵³ I sistemi contemplati dalla disposizione erano inizialmente classificati come sistemi di IA ad alto rischio, ma nel testo finale del regolamento sono stati inclusi tra le pratiche di IA vietate. Si veda al riguardo proposta di regolamento, del 21 aprile 2021, che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final.

persona fisica» in linea con la definizione di cui all'art. 4, par. 4, del regolamento (UE) 2016/679 (GDPR)⁵⁴.

Il riferimento è ai sistemi di c.d. *predictive policing* dei quali l'atto non fornisce una precisa definizione, ma che possono essere descritti come sistemi volti ad individuare e prevenire attività criminali attraverso l'analisi di dati complessi e l'elaborazione di previsioni in merito al compimento di reati e alla loro localizzazione (*place-based systems*) o all'elaborazione di profili criminali individuali (*person-based systems*)⁵⁵, utilizzando informazioni contenute in banche dati elaborate dalle forze dell'ordine, nei *social networks*, in Internet e negli impianti a circuito chiuso⁵⁶.

Questi strumenti presentano alcune criticità sia da un punto di vista qualitativo che quantitativo che impattano sulla tutela dei diritti umani. In primo luogo, l'individuazione di categorie di soggetti con un diverso grado di pericolosità (*social sorting*) implica rischi di stigmatizzazione. I *software* utilizzati dalle forze dell'ordine si basano spesso sui c.d. *dirty data*, vale a dire dati derivanti o in ogni caso influenzati da pregiudizi, cosicché questi sistemi tendono ad aver un effetto discriminatorio nei confronti di alcune categorie di soggetti, tra cui i migranti, causando molteplici forme di *bias* e di discriminazione⁵⁷. Ciò comporta conseguentemente il rischio di falsi positivi dovuti all'inaccuratezza dei dati processati, con l'effetto che *«low-quality data and/or low-quality procedures behind decision-making processes and*

⁵⁴ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

⁵⁵ S. Lonati, *Predictive policing: dal disincanto all'urgenza di un ripensamento*, in *Rivista di Diritto dei Media*, www.medialaws.eu, 30 settembre 2022. Inoltre, per approfondimenti sulle tipologie e le caratteristiche della polizia predittiva si rinvia a L.M. Sommerer, *Self-Imposed Algorithmic Thoughtlessness and the Automation of Crime Control. A Study of Person-Based Predictive Policing and the Algorithmic Turn*, Baden-Baden, 2022, p. 30 ss.

⁵⁶ Le strategie di polizia predittiva vengono infatti indicate come *«the use of data and analytics to predict crime»*, A.D. Selbst, *Disparate Impact in Big Data Policing*, in *Georgia Law Review*, 2017, p. 114. Inoltre, in argomento, T.W. Hung – C.P. Yen, *On the Person-Based Predictive Policing of AI*, in *Ethics and Information Technology*, 2021, p. 165, in cui si evidenzia che ciò che costituisce una novità in questo ambito non è l'uso della statistica, ma le nuove tecnologie che ricorrono ai big data che hanno modificato le caratteristiche di queste attività di law enforcement. Così anche E. Pietrocarlo, *La predictive policing nel regolamento europeo sull'intelligenza artificiale*, in *La legislazione penale*, 26 settembre 2024p. 3.

⁵⁷ Sul punto si veda S. Lonati, *op. cit.*; nonché *ex multis* e per altri riferimenti bibliografici P. Vogiatzoglou, *Mass Data Surveillance and Predictive Policing. Contested Foundations and Human Rights Impact*, New York, 2025.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

*analytical tools could result in biased algorithms, spurious correlations, errors, an underestimation of the legal, social and ethical implications»*⁵⁸. Eppure, la diffusione di queste attività di *law enforcement*⁵⁹ è dipesa proprio dalla crescente esigenza di sviluppare metodi di valutazione obiettivi, verificabili e, dunque, maggiormente affidabili rispetto alla *human intuition*⁶⁰, così da rendere le decisioni delle forze dell'ordine trasparenti e controllabili e da contrastare quelle pratiche discriminatorie intenzionali che caratterizzavano (e caratterizzano) la valutazione umana⁶¹. È chiaro quindi che l'impiego di questi sistemi impone di operare una valutazione del rapporto tra i benefici che possono offrire e gli impatti sui diritti umani che possono provocare, tra cui la dignità umana, il diritto alla non discriminazione, il diritto alla protezione dei dati e la tutela della *privacy*⁶², sanciti agli artt. 1, 7, 8 e 21 della Carta dei diritti fondamentali a cui il regolamento dichiara di voler garantire protezione⁶³.

Per quanto qui rileva, le preoccupazioni per i possibili effetti sui diritti menzionati appaiono significative nella misura in cui l'ultimo periodo della norma prevede un'esenzione dal suo ambito di applicazione dei sistemi di IA «utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa». In virtù di questa esenzione, i sistemi impiegati in funzione di supporto del processo decisionale umano, basato su fatti oggettivi e verificabili, non ricadono nell'alveo del divieto, ma nella categoria dei sistemi ad alto rischio, legittimandone dunque l'immissione, la messa a disposizione e l'utilizzo nell'ambito della migrazione, dell'asilo e della gestione dei controlli alle frontiere, come

⁵⁸ European Parliament, *Report on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-Discrimination, Security and Law-Enforcement*, 2016/2225(INI), 20 February 2017, par. M.

⁵⁹ S. Quattrocchio, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020, p. 131 ss.

⁶⁰ E. Pietrocarlo, *op. cit.*, p. 3.

⁶¹ A.D. Selbst, *op. cit.*, p. 120; W.S. Isaac, *Hope, Hype, and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice*, in *Ohio State Journal of Criminal Law*, 2018, p. 543-558.

⁶² J. Levano, *Predictive Policing in the AI Act: Meaningful Ban or Paper Tiger?*, in *European Law Blog*, www.europeanlawblog.eu, 5 July 2024.

⁶³ In tal senso, considerando 1 e art. 1 dell'*AI Act*.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

stabilito al par. 7 dell'Allegato III⁶⁴, seppur nel rispetto degli obblighi e dei requisiti stabiliti dal regolamento per questa categoria di sistemi⁶⁵.

Questa esenzione sembra essere giustificata dal valore aggiunto che la verifica condotta mediante un algoritmo predittivo potrebbe apportare alla valutazione umana⁶⁶. Tuttavia, la previsione non offre il necessario livello di chiarezza per la mancanza di sufficienti indicazioni in merito al criterio della «funzione di supporto alla valutazione umana» che ne costituisce il punto di riferimento fondamentale. La distinzione tra pratiche vietate e pratiche ad alto rischio dipende unicamente da questa funzione complementare che il sistema di IA svolge, risultando quindi dirimente stabilire se esso operi in modo esclusivamente automatico o meno. Tuttavia, la norma non chiarisce in modo sufficiente quale sia il livello di coinvolgimento umano richiesto per escludere un determinato sistema dall'applicazione del divieto in parola⁶⁷, aprendo alla possibilità che anche sistemi in cui tale coinvolgimento è *marginal and symbolic* possano essere ricondotti nella categoria dei sistemi che non sono vietati, ma sottoposti a stringenti obblighi di trasparenza e responsabilità⁶⁸ in quanto «semplicemente» considerati ad alto rischio.

Una (limitata) indicazione sul punto può ricavarsi dalle linee guida sulle pratiche vietate *ex art. 5* del regolamento sull'intelligenza artificiale pubblicate dalla Commissione europea il 4 febbraio 2025, pochi giorni dopo l'entrata in vigore del divieto, le quali, pur non essendo vincolanti, chiariscono l'interpretazione delle componenti della disposizione al fine di garantirne un'applicazione coerente, efficace e uniforme in tutta l'UE⁶⁹.

⁶⁴ E. Pietrocarlo, *op. cit.*, p. 20.

⁶⁵ Il par. 7 dell'Allegato III include infatti tra i sistemi di IA che possono essere impiegati nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere «i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti o per loro conto, oppure da istituzioni, organi e organismi dell'Unione, per valutare un rischio (compresi un rischio per la sicurezza, un rischio di migrazione irregolare o un rischio per la salute) posto da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro» (lett. b).

⁶⁶ E. Pietrocarlo, *op. cit.*, p. 30 ss.

⁶⁷ J. Laux, *Institutionalised Distrust and Human Oversight of Artificial Intelligence: Toward a Democratic Design of AI Governance under the European Union AI Act*, in *AI and Society*, 2024, p. 2853-2866.

⁶⁸ J. Levano, *op. cit.*

⁶⁹ European Commission, *Annex to the Communication to the Commission, Approval of the Content of the Draft Communication from the Commission – Commission Guidelines on Prohibited artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act)*, Bruxelles, 4 February 2025, C(2025) 884 final.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

La Commissione afferma che il concetto di «valutazione umana» andrebbe ricostruito ricorrendo alla giurisprudenza della CGUE, in specie a quanto stabilito nella nota sentenza *Ligue des droits* del 2022⁷⁰ in cui la Corte ha dichiarato che un sistema di sorveglianza continua, indiscriminata e sistematica, che include la valutazione automatizzata di dati personali comporta ingerenze gravi nei diritti garantiti dagli artt. 7 e 8 della Carta⁷¹ e che l'intervento umano con mezzi non automatizzati è indispensabile «al fine di identificare falsi positivi e garantire risultati non discriminatori»⁷². Il margine di errore che può derivare dall'analisi automatizzata pone pertanto l'esigenza di effettuare un riesame individuale non automatizzato del risultato ottenuto prima di adottare una misura che potrebbe avere effetti negativi sulla persona interessata⁷³.

Dunque, come indicato dalla Commissione, l'elemento centrale ai fini dell'esclusione dall'ambito di applicazione del divieto è che il sistema di IA venga utilizzato a supporto della valutazione umana «*rather than involving the AI system itself making the risk assessment as occurs in the situations covered by the prohibition*», purché tale valutazione sia già «*based on objective and verifiable facts directly linked to a criminal activity*»⁷⁴.

Pertanto, riteniamo che al fine di evitare l'elusione del divieto e garantirne l'efficacia, dovrebbe essere dimostrata l'esistenza di eventuali altri elementi «*real, substantial and meaningful*» per poter giustificare che il divieto non è applicabile⁷⁵. Ciò posto, un sistema di *predictive policing* utilizzato per prevedere il comportamento criminale, basandosi esclusivamente su caratteristiche personali, quali l'età o la nazionalità, considererà determinati individui più propensi «*to commit future offences that they have not yet committed*» e, come tale, si può presumere che sia vietato ai sensi dell'art. 5, par. 1, lett. d)⁷⁶.

Nonostante i chiarimenti della Commissione europea, in ogni caso l'art. 5, par. 1, lett. d) presenta considerevoli problematiche, soprattutto se letto alla luce della previsione di cui all'art. 2, par. 3 del regolamento che,

⁷⁰ Corte giust., 27 gennaio 2022, C-817/19, *Ligue des droits humains c. Conseil des ministers*.

⁷¹ *Ibid.*, punto 111.

⁷² European Commission, *Annex to the Communication to the Commission*, cit., p. 70.

⁷³ *Ligue des droits humains*, punto 124, nonché Corte giust., 6 ottobre 2020, C-511/18, *La Quadrature du Net*, punto 182.

⁷⁴ European Commission, *Annex to the Communication to the Commission*, cit., p. 71.

⁷⁵ *Ibid.*, p. 68.

⁷⁶ *Ibid.*, p. 69.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

stabilendo un'esenzione generale dall'applicazione dell'*AI Act* per ragioni di sicurezza nazionale⁷⁷, pone un limite significativo all'efficacia del divieto. Questa esenzione lascia di fatto un'ampia discrezionalità agli Stati membri in merito all'impiego di sistemi di IA, inclusi quelli di polizia predittiva, se si considera che il termine «sicurezza nazionale» è un concetto dal significato indefinito.

Sebbene questo aspetto richiederebbe ben altri approfondimenti, ci limitiamo qui a ricordare che, come noto, il TUE disciplina all'art. 4, par. 2 una clausola di salvaguardia della sovranità degli Stati membri in materia di sicurezza nazionale, introdotta con la riforma di Lisbona, stabilendo l'obbligo per l'Unione di rispettare «le funzioni essenziali dello Stato, tra cui le funzioni «di tutela della sicurezza nazionale» e che quest'ultima «resta di esclusiva competenza di ciascuno Stato membro»⁷⁸. Per quanto qui rileva, il diritto primario colloca la sicurezza nazionale tra i motivi di deroga alla libera circolazione delle persone nell'ambito dello Spazio di libertà, sicurezza e giustizia. A tal proposito, l'art. 72 TFUE stabilisce che le disposizioni del Titolo V del Trattato non ostano «all'esercizio delle responsabilità incumbenti agli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna», riconoscendo un certo margine di discrezionalità agli Stati membri in merito all'applicazione di

⁷⁷ Si legge, infatti, che «[I]l presente regolamento non si applica a settori che non rientrano nell'ambito di applicazione del diritto dell'Unione e, in ogni caso, non pregiudica le competenze degli Stati membri in materia di sicurezza nazionale, indipendentemente dal tipo di entità incaricata dagli Stati membri di svolgere compiti in relazione a tali competenze. Il presente regolamento non si applica ai sistemi di IA se e nella misura in cui sono immessi sul mercato, messi in servizio o utilizzati con o senza modifiche esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività. Il presente regolamento non si applica ai sistemi di IA che non sono immessi sul mercato o messi in servizio nell'Unione, qualora l'output sia utilizzato nell'Unione esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività».

⁷⁸ La bibliografia sul tema è amplissima. Si vedano, segnatamente, S. Peers, *National Security and European Law*, in *Yearbook of European Law*, 1999, pp. 363 ss.; M.C. Baruffi, *Art. 4 TUE*, in F. Pocar – M.C. Baruffi (a cura di), *Commentario breve ai Trattati dell'Unione europea*, Padova, 2014, pp. 13-24; S. Pugliese, *L'evoluzione della nozione di sicurezza dell'Unione europea tra crisi sistemiche, innovazioni tecnologiche e tutela dei valori*, Bari, 2025. Si vedano, inoltre, inoltre, le Conclusioni dell'Avvocato generale M. Poiras Maduro, presentate l'8 ottobre 2008, C-213/07, *Michaniki AE*, punto 31.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

misure derogatorie nazionali purché siano limitate a quanto strettamente necessario⁷⁹.

D'altro canto, la Corte di giustizia, nella sentenza *Commissione c. Polonia, Ungheria e Repubblica ceca*⁸⁰, ha chiarito che l'art. 72 TFUE «in quanto disposizione derogatoria, [...] non conferisce agli Stati membri il potere di derogare a disposizioni di diritto dell'Unione mediante il mero richiamo agli interessi connessi al mantenimento dell'ordine pubblico e alla salvaguardia della sicurezza interna, ma impone loro di dimostrare la necessità di avvalersi della deroga prevista da tale articolo al fine di esercitare le loro responsabilità in tali materie». Peraltro, secondo sua costante giurisprudenza «anche se spetta agli Stati membri stabilire le misure adeguate per garantire l'ordine pubblico nel loro territorio nonché la loro sicurezza interna ed esterna» le deroghe espresse «riguardano ipotesi eccezionali chiaramente delimitate» da cui «non è lecito dedurre una riserva generale [...] che escluda dall'ambito d'applicazione del diritto dell'Unione qualsiasi provvedimento» adottato per queste ragioni in quanto «rischierebbe di compromettere la forza cogente e l'applicazione uniforme del diritto dell'Unione»⁸¹. La sicurezza nazionale fa quindi riferimento «all'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società e comprende la prevenzione e la repressione di attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali

⁷⁹ G. Naddeo, *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella «data retention saga» dinanzi alla Corte di giustizia UE*, in *Freedom, Security and Justice: European Legal Studies*, 2022, p. 188-217. In tema di bilanciamento tra sicurezza nazionale e diritti fondamentali si veda G. Martinico, *What lies behind article 4(2) TEU?*, in A.S. Arnaiz – C.A. Llivina (eds.), *National Constitutional Identity and European Integration*, Louvain-la-Neuve, 2013, p. 93 ss.; G. de Vergottini, *Una rilettura del concetto di sicurezza nell'era digitale e dell'emergenza normalizzata*, in *Rivista AIC*, 2019, p. 65-85; X. Dupré de Boulois, *Existe-t-il un droit fondamental à la sécurité ?*, in *Revue des droits et libertés fondamentaux*, 2018, p. 1-11; F. Ferraro, *Brevi note sulla competenza esclusiva degli Stati membri in materia di sicurezza nazionale*, in A.V. V.V., *Annali AISDUE*, Bari, 2020, p. 117 ss.; M. Claes, *National Identity and the Protection of Fundamental Rights*, in *European Public Law*, 2021, p. 517 ss.; S. Crespi, *L'influenza del diritto dell'Unione europea sulla sicurezza nazionale: l'art. 4, par. 2, TUE alla prova della recente giurisprudenza UE tra l'altro in materia di privacy*, in *Eurojus*, 2022, p. 85-111.

⁸⁰ Corte giust., 2 aprile 2020, C-715/17, C-718/17, C-719/17, *Commissione c. Polonia, Ungheria e Repubblica ceca*, punto 152.

⁸¹ *Ibid.*, punto 143. Si vedano, inoltre, le sentenze della Corte giust., 15 dicembre 2009, C-461/05, *Commissione c. Danimarca*, punto 51 e 4 marzo 2010, C-38/06, *Commissione c. Portogallo*, punto 62 e giurisprudenza ivi citata.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

fondamentali di un paese»⁸², tesa per l'appunto a salvaguardare le funzioni essenziali dello Stato da minacce di eccezionale gravità, e costituisce un «obiettivo d'interesse generale» dell'Unione europea⁸³.

Tuttavia, la questione appare rilevante nella misura in cui il crescente e diffuso ricorso a sistemi di *predictive policing* a fini di prevenzione e contrasto avverso possibili minacce, qualora impiegati nell'ambito dei controlli alle frontiere esterne, possa essere giustificato quale «misura derogatoria» necessaria per assicurare la salvaguardia della sicurezza nazionale, sollevando non pochi dubbi in ordine al grado di invasività nei diritti fondamentali dei migranti che potrebbero determinare, come da più parti sostenuto⁸⁴. In altri termini, il timore è che l'esenzione legata alla sicurezza nazionale possa essere invocata per giustificare l'uso dei sistemi in esame con il pretesto di salvaguardare la sicurezza nazionale, con il rischio conseguente di minare l'efficacia del divieto e di dar vita a gravi violazioni dei diritti fondamentali in gioco e a gravi esiti discriminatori, a partire dal rifiuto di ingresso nel territorio dell'Unione⁸⁵.

3.2 *Segue: art. 5, par. 1, lett. f) e divieto dei sistemi di riconoscimento delle emozioni: an obvious loophole nel settore dei controlli alle frontiere?*

Un esempio paradigmatico dell'errata classificazione concerne i sistemi di «riconoscimento delle emozioni» (*facial emotion recognition* o FER)⁸⁶ ovvero tecnologie che impiegano svariate tecniche, come l'analisi dei lineamenti del viso, del tono di voce, del linguaggio, ecc., per rilevare le caratteristiche fisiche, fisiologiche o comportamentali delle persone fisiche

⁸² *La Quadrature du Net*, punto 135; sentenza del 6 ottobre 2020, C-623/17, *Privacy International*, punto 74; sentenza del 20 settembre 2022, C-793/19 e C-794/19, *SpaceNet*, punto 92.

⁸³ S. Crespi, *op. cit.*

⁸⁴ Article 19, *EU: AI Act Fails to Set Gold Standard for Human Rights*, www.article19.org, 4 April 2024; AccessNow, *The EU AI Act: A Failure for Human Rights, a Victory for Industry and Law Enforcement*, www.accessnow.org, 13 March 2024.

⁸⁵ J. Levano, *op. cit.*

⁸⁶ La *facial emotion recognition* fa parte delle tecnologie del c.d. *affective computing*, un campo di ricerca multidisciplinare sulle capacità dei computer di riconoscere e interpretare le emozioni umane attraverso l'analisi delle emozioni ricavate a partire da immagini e video. Sul tema e per ulteriori riferimenti bibliografici si rinvia, segnatamente, a R.A. Calvo – S. D'Mello – J. Gratch – A. Kappas, *The Oxford Handbook of Affective Computing*, Oxford, 2015.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

(o c.d. bio-caratteristiche) e identificarne le emozioni⁸⁷. Questi sistemi implicano, da un lato, un processo di «datificazione» delle emozioni umane, e dall'altro, una categorizzazione delle persone fisiche sulla base delle loro emozioni⁸⁸. Le emozioni sono infatti considerate come uno strumento per determinarne la personalità e l'identità, con lo scopo di costruire il profilo di una persona fisica e di prevederne il comportamento⁸⁹.

L'art. 3, par. 39, del regolamento definisce un sistema di riconoscimento delle emozioni come un «sistema di IA finalizzato all'identificazione o all'inferenza di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici». In particolare, come chiarito nel considerando 18, la nozione fa riferimento «a emozioni o intenzioni quali felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento. Non comprende stati fisici, quali dolore o affaticamento [...]. Non comprende neppure la semplice individuazione di espressioni, gesti o movimenti immediatamente evidenti, a meno che non siano utilizzati per identificare o inferire emozioni».

Orbene, l'art. 5, par. 1, lett. f), include tra le pratiche vietate, perché considerate inaccettabili, i sistemi di «riconoscimento delle emozioni» di una persona fisica, ma ne circoscrive tuttavia l'applicazione a due ambiti ben precisi e prevedendo alcune eccezioni non molto chiare: il divieto trova infatti applicazione solo in riferimento all'ambito lavorativo e a quello scolastico, salvo poi che un simile sistema sia destinato a essere implementato o immesso sul mercato per motivi medici o di sicurezza. Se ne deduce, quindi, la possibile applicazione nel contesto della migrazione e dei controlli alle frontiere.

Le problematiche derivanti dall'esclusione del settore della migrazione e dei controlli alle frontiere dall'ambito di applicazione del divieto in parola dipendono innanzitutto da questioni di natura etica, data la

⁸⁷ P. Filippi, *Emotion Communication through Voice Modulation: Insights on Biological and Evolutionary Underpinnings of Language*. *Theoria et Historia Scientiarum*, 2019, p. 83 ss.; J. Buolamwini – V. Ordóñez – J. Morgenstern – E. Learned-Miller, *Facial Recognition Technologies: A Primer*, p. 4-5, www.people.cs.umass.edu, 29 May 2020; T.M. Wani et al., *A Comprehensive Review of Speech Emotion Recognition Systems*, in *IEEE Access*, p. 47795 ss., www.iris.uniroma1.it, 2021; S. Pal – S. Mukhopadhyay – N. Suryadevara, *Development and Progress in Sensors and Technologies for Human Emotion Recognition*, in *Sensors*, 2021, p. 5554 ss.

⁸⁸ H. Ruschemeier, *Data Broker and European Digital Legislation*, in *EDPL - European Data Protection Legislation*, 2023, p. 27-38; R. Montinaro, *Riconoscimento delle emozioni e marketing personalizzato*, in *Persona e Mercato*, 2024, p. 849.

⁸⁹ R. Montinaro, *op. cit.*, p. 850.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

difficoltà di stabilire cosa sia un'emozione⁹⁰, e dalla dubbia accuratezza di simili sistemi⁹¹, nonché dalla circostanza che il rilevamento delle emozioni costituisce di fatto una vera e propria forma di «sorveglianza altamente invasiva». Tale forma di sorveglianza «*involves the mass collection of sensitive personal data in invisible and unaccountable ways, enabling the tracking, monitoring, and profiling of individuals, often in real time*»⁹², trattandosi di tecnologie pseudoscientifiche⁹³, che deducono le emozioni utilizzando i dati biometrici di un individuo, considerate scientificamente discutibili e fondamentalmente incompatibili con alcuni diritti umani fondamentali⁹⁴. Il ricorso a questi sistemi tende infatti a rafforzare un processo di *racialized suspicion* nei confronti dei migranti e ad automatizzare *discriminatory assumptions*⁹⁵.

A ben vedere, con gli emendamenti proposti dal Parlamento europeo all'AI Act nel corso del complesso iter legislativo che ne ha preceduto la

⁹⁰ European Parliament, *Regulating Facial Recognition in the EU*, p. 4, www.europarl.europa.eu, September 2021.

⁹¹ E. Selinger, *AI Can't Detect our Emotions*, in *Medium*, www.onezero.medium.com, 6 April 2021. La gran parte degli strumenti di riconoscimento delle emozioni si basa, infatti, sulla controversa teoria delle *basic emotions* di Paul Ekman, che individua *universal categories of basic emotions* e indica come queste possano essere dedotte a partire dalle espressioni facciali, P. Ekman, *Basic Emotions*, in T. Dalgleish – M. Power (eds.), *Handbook of Cognition and Emotions*, New York, 1999, p. 45 ss. Tuttavia, non solo il riconoscimento delle emozioni è un processo molto più complesso, dipendente da fattori di varia natura, ma sussistono seri dubbi sulla capacità dei sistemi attuali, e persino di quelli futuri, di realizzare effettivamente ciò che promettono. Al riguardo, si vedano, *ex multis*, K. Kryszewski et al., *Be Careful Where You Smile: Culture Shapes Judgments of Intelligence and Honesty of Smiling Individuals*, in *Journal of Nonverbal Behaviour*, 2015, p. 101-116; L. Feldman Barrett – R. Adolphs – S.D. Pollak – S. Marsella – A.M. Martinez, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, in *Psychological Science in the Public Interest*, 2019, pp. 1-68; A. Korte, *Facial-Recognition Technologies Cannot Read Emotions, Scientists Say*, in *American Association for the Advancement of Science*, www.aaas.org, 6 April 2021.

⁹² Article 19, *Emotional Entanglement: China's Emotion Recognition Market and its Implications for Human Rights*, London, p. 15, www.article19.org, 2021.

⁹³ F. Cabitza – A. Campagner – M. Mattioli, *The Unbearable (Technical) Unreliability of Automated Facial Emotion Recognition*, in *Big Data and Society*, 2022, p. 1-17; V. Marda – E. Jakubowska, *Emotion (Mis)Recognition: is the EU Missing the Point?*, in *European Digital Rights (EDRi)*, www.edri.org, 2 February 2023; J. Kanestrøm, *Is it Acceptable for Artificial Intelligence to Read Your Emotions?*, in *Research News from the University of Oslo*, www.uio.no, 21 January 2025.

⁹⁴ V. Marda – E. Jakubowska, *op. cit.*

⁹⁵ Access Now et al., *The EU AI Act Must Protect People on the Move*, www.edri.org, 6 February 2023.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

definitiva adozione⁹⁶, sembrano essere state colte ed accolte le criticità evidenziate. Ed infatti, queste preoccupazioni risultano condivise ove si consideri che nel considerando 44 dell'atto vengono evidenziati i seri timori in merito «alla base scientifica dei sistemi di IA volti a identificare o inferire emozioni, in particolare perché l'espressione delle emozioni varia notevolmente in base alle culture e alle situazioni e persino in relazione a una stessa persona». Questi sistemi vengono infatti considerati carenti a causa della limitata affidabilità, della mancanza di specificità e della limitata generalizzabilità e perché, utilizzando i dati biometrici per identificare o inferire le emozioni, possono determinare «risultati discriminatori e possono essere invasivi dei diritti e delle libertà delle persone interessate», nonché «determinare un trattamento pregiudizievole o sfavorevole» (considerando 44).

Ciononostante, queste preoccupazioni non sembrano estendersi al settore migratorio, alla luce dell'esenzione prevista dall'art. 5, par. 1, lett. f). Al contrario, riteniamo che la possibilità di utilizzare questi sistemi nel contesto in esame non tenga conto dell'evidente effetto che potrebbero avere per i migranti, trattandosi di sistemi il cui impatto «*can be life changing*»⁹⁷, in particolare per il godimento di alcuni diritti fondamentali, in primis il diritto alla protezione dei dati personali sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea, ma anche perché potenzialmente in grado di violare il principio di non-refoulement alla frontiera.

Peraltro, viene in rilievo un'ulteriore criticità legata al rischio di violazione che potrebbe derivare dall'impiego di sistemi di riconoscimento delle emozioni degli emergenti «neurodiritti»⁹⁸. Questi possono essere definiti «*as ethical, legal, social or natural principles of freedom or entitlement related to a person's cerebral and mental domains*»⁹⁹ e sarebbero diretti a garantire la protezione di quella che viene definita *mental privacy* che denota l'ambito dei processi e delle esperienze cerebrali attivi di una persona, quali

⁹⁶ European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), P9_TA(2023)0236.

⁹⁷ IOM, *World Migration Report 2022*, Geneva, p. 16 ss., www.publications.iom.int, 2022.

⁹⁸ M. Tuozzo, *Note intorno al (futuro) Artificial Intelligence Act. Prospettive costituzionali e sfide dell'immigrazione nell'ecosistema digitale*, in *Diritto pubblico europeo*, 2024, p. 221 ss.

⁹⁹ European Parliament, *The Protection of Mental Privacy in the Area of Neuroscience. Societal, Legal and Ethical Challenges*, p. 38 ss., www.europarl.europa.eu, July 2024.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

percezioni, pensieri, emozioni, volontà¹⁰⁰ dalle neuroscienze, dalle neurotecnologie e da quella branca dell'intelligenza artificiale dedita allo sviluppo di sistemi di comprensione scientifica dei processi cerebrali¹⁰¹.

Il riferimento è alle possibili violazioni che potrebbero derivarne per la «libertà cognitiva» dell'individuo, vale a dire la sua capacità di esercitare il controllo sulla propria coscienza, minandone l'autonomia personale e la dignità¹⁰², e quindi per il diritto «to mental self-determination guarantees individuals sovereignty over their minds»¹⁰³.

Posto che le questioni aperte dall'emersione di questa nuova categoria di diritti e della libertà cognitiva rimangono ancora ampiamente inesplorate in dottrina non possono ignorarsi le implicazioni che i sistemi di riconoscimento delle emozioni potrebbero determinare anche per i neurodiritti dei cittadini di Paesi terzi interessati dai controlli di gestione delle frontiere dell'UE sempre più affidati a questi sistemi.

Di conseguenza, la mancata estensione del divieto di cui all'art. 5, par. 1, lett. f) al settore della gestione della migrazione e del controllo alle frontiere non sorprende, se si considera che da tempo l'UE sta sostenendo ingenti investimenti¹⁰⁴ nella ricerca e sviluppo di poligrafi, lie detectors e sistemi di riconoscimento facciale e delle emozioni¹⁰⁵ a fini di controllo degli

¹⁰⁰ P. Kellmeyer, «Neurorights». *A Human Rights-Based Approach for Governing Neurotechnologies*, in S. Voenecky – P. Kellmeyer – O. Mueller – W. Burgard (eds.), *The Cambridge Handbook of Responsible Artificial Intelligence. Interdisciplinary Perspectives*, Cambridge, 2022, p. 414 ss.

¹⁰¹ *Ibid.*, p. 412. Inoltre, sul tema si rinvia a N. Hertz, *Neurorights – Do we Need new Human Rights? A Reconsideration of the Right to Freedom of Thought*, in *Neuroethics*, 2023, p. 1-15; UNESCO, *The Risks and Challenges of Neurotechnologies for Human Rights*, Milano-New York, 2023; C. Bublitz, *Neurotechnologies and Human Rights: Restating and Reaffirming the Multi-Layered Protection of the Person*, in *The International Journal of Human Rights*, 2024, p. 782-807.

¹⁰² M. Ienca, *On Artificial Intelligence and Manipulation*, in *Topoi*, 2023, p. 833-842, in particolare p. 838.

¹⁰³ J.C. Bublitz, *My Mind is Mine!? Cognitive Liberty as a Legal Concept*, in E. Hildt – A. Francke (eds.), *Cognitive Enhancement*, Cham, 2013, p. 233-264, in specie p. 242.

¹⁰⁴ Sugli investimenti nello sviluppo di sistemi di IA per il controllo dell'immigrazione da parte dell'Unione europea si veda S. Penasa, *Intelligenza artificiale e diritti: verso un diritto «algoritmico» dell'immigrazione?*, in F. Biondi Dal Monte – M. Forti – L. Ranieri (a cura di), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa*, Roma, 2024, p. 17-48.

¹⁰⁵ Al riguardo si veda European Parliament, *Migration and Border Management. Heading 4 of the 2021-2027 MFF*, www.europarl.europa.eu, April 2021; Statewatch, *EU Has Spent over €340 Million on Border AI Technology that New Law Fails to Regulate*, www.statewatch.org, 12 May 2022.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

attraversamenti dei suoi confini esterni, nonostante i problemi rilevati. Un'esclusione che trova peraltro conferma nelle citate linee guida della Commissione europea che, nell'indicare quali sistemi non rientrano nel campo di applicazione della norma, chiarisce che i sistemi di riconoscimento delle emozioni utilizzati in tutti gli altri ambiti, ad eccezione del mondo del lavoro e degli istituti scolastici, non rientrano nel divieto di cui all'art. 5, par. 1, lett. f), ma sono considerati ad alto rischio e possono essere vietati solo in determinate circostanze ovvero se ricadano nei divieti definiti nelle lett. a) e b) del par. 1 dell'art. 5¹⁰⁶. Questa impostazione tende dunque a confermare l'idea che con il regolamento sull'intelligenza artificiale sia stato creato un quadro giuridico parallelo per l'impiego dei sistemi di IA nel settore della gestione della migrazione e dei controlli alle frontiere¹⁰⁷.

3.3 *Segue: esenzione dei sistemi di categorizzazione biometrica utilizzati nelle attività di contrasto e rischi di violazione del diritto alla protezione dei dati personali dei migranti per esigenze di sicurezza.*

Un'ultima, significativa esenzione che rileva nell'ambito della presente analisi è quella prevista dalla successiva lett. g) del par. 1 dell'art. 5 del regolamento (UE) 2024/1689 con riferimento ai sistemi di categorizzazione biometrica.

La disposizione sancisce il divieto di immissione, messa in servizio o uso di «sistemi di categorizzazione biometrica» – vale a dire sistemi che utilizzano «i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche» (art. 3, par. 40) – che «classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale», specificando però che tale divieto non si estende ai sistemi di etichettatura o filtraggio «di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto» che, anche in questo caso, rientreranno tra i sistemi ad alto rischio dell'Allegato III.

La categorizzazione biometrica che, come noto, ha lo scopo di stabilire l'appartenenza di un individuo ad una precisa categoria di persone

¹⁰⁶ European Commission, *Annex to the Communication to the Commission*, cit., p. 89.

¹⁰⁷ In tal senso, si veda AccessNow, *Joint Statement – A Dangerous Precedent: How the EU AI Act Fails Migrants and People on the Move*, www.accessnow.org, 13 March 2024.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

sulla base di una caratteristica predefinita, è sottratta all'applicazione del divieto nell'ambito delle attività di contrasto che, in base a quanto indicato dall'art. 3, par. 45 del regolamento, comprendono tutte quelle attività svolte dalle «autorità di contrasto o per loro conto a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse»¹⁰⁸.

È da evidenziare che il regolamento sull'intelligenza artificiale, riprendendo quasi pedissequamente la definizione di cui all'art. 4, par. 14, del regolamento (UE) 2016/679 (GDPR)¹⁰⁹, qualifica i dati biometrici come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici» (art. 3, par. 34). Come noto, i dati biometrici costituiscono una categoria particolare di dati personali¹¹⁰, la cui specificità è basata sul processo di estrazione ovvero sul trattamento tecnico specifico concernente determinate caratteristiche della persona¹¹¹, e

¹⁰⁸ Le autorità di contrasto cui fa riferimento il regolamento includono «a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse; oppure b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse».

¹⁰⁹ «Dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici», Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

¹¹⁰ Ai sensi dell'art. 4, par. 1 del GDPR per «dato personale» si intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

¹¹¹ G. Contaldi, *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, 2021, p. 1193-1213; A.C. Nazzaro, *La tutela dei dati biometrici tra GDPR e AI Act*, in *European Journal of Privacy Law and Technology*, 2024, p. 37-53.

rientrano nel novero dei c.d. «dati sensibili» di cui al par. 1, dell'art. 9, GDPR.

Tali dati possono essere utilizzati per molteplici scopi¹¹², inclusa la lotta alle attività criminali e avverso possibili minacce alla sicurezza pubblica da parte delle forze dell'ordine¹¹³. Tuttavia, la gran parte di questi strumenti si basa sul trattamento automatizzato dei dati in parola; il che solleva non poche perplessità sulla loro effettiva capacità di tutelare gli interessati da possibili ingerenze con diritti considerati fondamentali, quali il diritto alla protezione dei dati personali di cui all'art. 8 della Carta di Nizza e il diritto al rispetto della vita privata di cui all'art. 7.

Questa previsione appare particolarmente significativa in un contesto come quello dei controlli alle frontiere se si considera che gli attori impegnati nella gestione dei controlli si ritrovano a trattare una quantità indefinita di dati biometrici dei migranti anche (e soprattutto) al fine di garantire una maggiore sicurezza dei Paesi di destinazione. La categorizzazione biometrica basata sull'etichettatura o il filtraggio di set di dati biometrici cui fa riferimento l'art. 5, par. 1, lett. g) dell'AI Act costituisce infatti una forma di trattamento automatizzato di dati biometrici.

Trattandosi, come detto, di dati sensibili, in linea di principio ne è vietato o limitato il trattamento¹¹⁴, salvo che ricorra una delle condizioni specificamente indicate al par. 2 dell'art. 9 GDPR¹¹⁵, ad esempio quando «necessario per motivi di interesse pubblico» purché il trattamento risulti «proporzionato alla finalità perseguita» e avvenga nel rispetto della «essenza del diritto alla protezione dei dati» e prevedendo «misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato» (lett. g), posto che il regolamento sull'IA non pregiudica l'applicazione del vigente diritto dell'Unione in tema di trattamento dei dati personali. Con riferimento a questa tipologia di dati, che consentono di identificare una persona fisica o ne confermano l'identificazione, la liceità del trattamento è

¹¹² E. Brouwer, *Digital Borders and Real Rights. Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden-Boston, 2008, p. 137 ss.

¹¹³ M. Forti, *Flussi migratori e protezione dei dati personali: alla ricerca di un punto di equilibrio tra sicurezza pubblica e tutela della privacy dei migranti e dei rifugiati all'interno del territorio europeo*, in *Rivista di diritto dei media*, 2020, p. 212-230.

¹¹⁴ «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

¹¹⁵ L'art. 9, par. 2 del GDPR indica nelle lettere da a) a j) in quali casi il par. 1 non si applica.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

ancorata al requisito del consenso dell'interessato o, in alternativa (e per quanto qui rileva) al criterio della necessità.

Poste tali premesse, ciò che si teme è che il ricorso a sistemi di categorizzazione biometrica nell'ambito dei controlli alle frontiere potrebbe farsi rientrare nell'alveo di tale deroga, alla luce di sopravvenute esigenze di tutela della sicurezza pubblica. È pur vero che tale deroga prevede che sia assicurata la protezione dei diritti fondamentali e i principi sanciti dal GDPR. Infatti, come stabilito dall'art. 5 GDPR, che indica quali sono i principi che devono informare il trattamento dei dati personali (liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; minimizzazione della conservazione; integrità e riservatezza; responsabilizzazione), il trattamento deve avvenire in modo da prevenire, o perlomeno minimizzare, eventuali rischi per i diritti fondamentali delle persone fisiche¹¹⁶.

Viene quindi in rilievo il profilo delle limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta dei diritti fondamentali. In particolare, conformemente al dettato dell'art. 52, par. 1, della Carta eventuali limitazioni all'esercizio dei diritti e delle libertà ivi sanciti «devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà» e quindi, alla luce del principio di proporzionalità, non devono andare oltre quanto strettamente necessario e rispondere a finalità di interesse generale¹¹⁷.

Il che trova conferma anzitutto nella giurisprudenza della CGUE, la quale ha più volte precisato che, trattandosi di una categoria particolare di dati sensibili, il relativo trattamento può essere considerato lecito solo qualora l'ingerenza nei suddetti diritti e le relative limitazioni non vadano oltre quanto «strettamente necessario», risultando quindi escluso qualsiasi trattamento di carattere generale o sistematico¹¹⁸. Inoltre, sul punto è

¹¹⁶ R. Bendinelli, *Le norme sul trattamento dei dati personali dei richiedenti asilo nell'Unione europea: talune criticità rispetto al caso dell'interessato minorenni*, in *Diritto, Immigrazione e Cittadinanza*, 2024, p. 8.

¹¹⁷ F. Mollo, *Il trattamento dei dati biometrici nell'AI Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale*, p. 112 ss, www.federalismi.it, 2024.

¹¹⁸ Si veda, da ultimo, Corte giust., 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland*, in cui si legge che «conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti da quest'ultima devono essere previste dalla legge, rispettare il loro contenuto essenziale e, nel rispetto del principio di proporzionalità, possono essere apportate limitazioni a detti diritti e libertà solo laddove

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

intervenuta anche la Corte europea dei diritti dell'uomo (Corte EDU) a più riprese. Richiamando l'art. 8 della Convenzione europea dei diritti dell'uomo sul diritto al rispetto della vita privata e familiare¹¹⁹, ha chiarito che «un'ingerenza [nel diritto al rispetto della vita privata e familiare] può essere giustificata ai sensi dell'articolo 8, paragrafo 2 [della Convenzione europea dei diritti dell'uomo], solo se essa è conforme alla legge, se persegue uno o più degli obiettivi legittimi a cui si riferisce il paragrafo 2 dell'articolo 8 e se è necessaria in una società democratica per raggiungere tali obiettivi»¹²⁰. La Corte EDU ha inoltre chiarito che le ingerenze con questo diritto possono essere giustificate solo per ragioni di necessità nazionale e, pur attribuendo un'ampia discrezionalità alle autorità competenti per la valutazione della necessità di una eventuale ingerenza per ragioni di sicurezza, ciò non può giustificare illegittime violazioni dei diritti fondamentali degli interessati¹²¹.

Tuttavia, i dati biometrici oggetto di categorizzazione riguardanti i migranti che giungono ai confini dell'Unione vengono generalmente raccolti e conservati in appositi database al fine di poter accertare in qualunque momento se costituiscano o meno una minaccia per la sicurezza, aprendo al chiaro rischio di una possibile profilazione del migrante in grado di incidere sul godimento di alcuni dei suoi diritti fondamentali nonché su eventuali decisioni relative al rilascio del visto e del permesso di soggiorno. A tal proposito, l'art. 22 GDPR stabilisce il diritto a «non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». Sebbene tale diritto venga meno ai sensi del par. 2, lett. b) dell'art. 22 GDPR qualora il processo decisionale automatizzato sia autorizzato «dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento», devono in ogni caso

siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui», punto 38.

¹¹⁹ «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui», Convenzione europea dei diritti dell'uomo, 4 dicembre 1950.

¹²⁰ Corte EDU, 4 luglio 2023, ric. 11519/20, *Glukhin v. Russia*, par. 75.

¹²¹ Si veda, *ex multis*, Corte EDU, 26 marzo 1987, ric. 9248/81, *Leander c. Svezia*, 22 settembre 1993, ric. 15473/89, *Klaas c. Germania*. Inoltre, in dottrina, E. Brouwer, *op. cit.*, p. 173 ss.; M. Forti, *op. cit.*, p. 217 ss.

essere previste «misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

In conclusione, ciò che si teme è che l'esenzione prevista dall'art. 5, par. 1, lett. g) dell'AI Act non sia in grado di assicurare il necessario bilanciamento tra le esigenze di salvaguardia avverso eventuali minacce che caratterizzano le attività di contrasto cui fa riferimento e la necessità di impedire la violazione del diritto alla protezione dei dati anche nei confronti dei migranti che, arrivati alle frontiere, vengono sottoposti a simili controlli¹²².

4. Conclusioni.

Il rafforzamento dei confini europei è sempre più intrinsecamente legato all'uso delle tecnologie digitali, in specie ai sistemi di intelligenza artificiale. Dai passaporti biometrici e gli *Automated Border Control systems* (ABC)¹²³ ai droni, ai sensori e alle tecnologie di rilevamento utilizzate per prevenire e individuare i migranti irregolari, le tecnologie digitali sono diventate una componente chiave della politica migratoria europea e del processo di costruzione della "Fortezza Europa". Solo tra il 2014 e il 2022, l'UE ha stanziato oltre 250 milioni di euro per la realizzazione di 49 progetti volti a sviluppare tecnologie di frontiera¹²⁴ e con l'imminente presentazione

¹²² Sul tema della tutela accordata dal GDPR ai migranti e richiedenti protezione internazionale si veda R. Bendinelli, *op. cit.*; M. Forti, *op. cit.*; V. Ferraris, *Eurodac e i limiti della legge: quando il diritto alla protezione dei dati personali non esiste*, in *Diritto, Immigrazione e Cittadinanza*, 2017, p. 1-16; B. Hayes, *Migration and Data Protection: Doing no Harm in an Age of Mass Displacement, Mass Surveillance and «Big Data»*, in *International Review of the Red Cross*, 2017, p. 179 ss.; M. Orofino, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Rivista di diritto dei media*, 2017, p. 82-104.

¹²³ I sistemi ABC sono progettati per sostituire i controlli manuali dei passaporti, richiedendo ai viaggiatori di inserire il passaporto in uno scanner, che cattura un'immagine della pagina con la foto. Il sistema scatta quindi una foto in tempo reale del volto del passeggero, la confronta con l'immagine del passaporto e, se l'algoritmo rileva una corrispondenza, il varco si apre automaticamente. Nell'Unione europea questi sistemi (come ABC4EU), sono finanziati nell'ambito del programma di ricerca *Horizon* e sono stati introdotti come progetti pilota, al fine di testare i miglioramenti che apportano all'identificazione dei passeggeri ai valichi di frontiera in termini di velocità, sicurezza e automazione di alcune azioni durante i controlli di frontiera. Informazioni dettagliate sul sistema ABC4EU sono disponibili sul sito: www.cordis.europa.eu.

¹²⁴ Statewatch, *Automating the Fortress: Digital Technologies and European Borders*, www.statewatch.org, 6 June 2024.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

del nuovo bilancio dell'Unione per il periodo 2028-2034, ciò che si prospetta è «*an increase of funds available for migration [...] in several areas, including [...] the so-called innovative solutions*»¹²⁵.

L'adozione del regolamento sull'intelligenza artificiale ha costituito senza dubbio «*a pivotal moment*»¹²⁶ nella regolamentazione dei sistemi di IA impiegati nell'UE, inclusi quelli impiegati nel contesto migratorio e della gestione delle frontiere. Ispirandosi ad un approccio *risk-based*, si è detto che il regolamento classifica i sistemi di IA secondo «una struttura piramidale a rischio crescente»¹²⁷ suddivisa in quattro distinti livelli di rischio dipendenti dall'uso di un dato sistema. Tra questi, l'art. 5, in vigore dal 2 febbraio 2025, stabilisce un divieto di immissione, messa in servizio ed utilizzo di quelle pratiche che sono considerate «inaccettabili» a causa della loro contrarietà ai valori dell'Unione, quali il rispetto della dignità umana, la libertà, l'uguaglianza, nonché i diritti fondamentali sanciti dalla Carta, compresi il diritto alla non discriminazione, alla protezione dei dati e alla vita privata e i diritti dei minori.

Ciononostante, come è stato osservato, la previsione di una serie di deroghe all'applicazione del divieto, in specie nel settore del controllo alle frontiere, sembra andare in senso contrario all'intento dichiarato di voler istituire «un sistema di regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione dell'IA nel mercato interno, garantendo nel contempo un elevato livello di protezione degli interessi pubblici, quali [...] la protezione dei diritti fondamentali» (considerando 8).

L'esenzione di cui alla lett. d) del par. 1, art. 5 concernente i sistemi di *predictive policing* mina notevolmente l'efficacia del divieto, che risulta indebolito dalla possibilità di un utilizzo dei sistemi in parola basata sulla funzione complementare rispetto alla valutazione umana, di cui non sono ben chiari la portata ed il significato, o in alternativa, su esigenze di sicurezza nazionale, lasciando di fatto alle autorità interessate, nel primo caso, e agli Stati membri, nel secondo, un'ampia discrezionalità in merito al ricorso a sistemi predittivi di scarsa affidabilità per i rischi di stigmatizzazione e discriminazione cui possono dar vita. L'insieme di questi aspetti ridimensiona significativamente la portata del divieto, ostacolando una

¹²⁵ Council of the European Union, *Making the Best Use of the Financial Framework for Enhancing Comprehensive Cooperation on the External Dimension of Migration and Asylum*, Bruxelles, 12 June 2025, 9372/25, p. 5.

¹²⁶ N. Vavoula, *Regulating AI at EU's Borders*, cit.

¹²⁷ F. Mollo, *op. cit.*, p. 101.

tutela sostanziale dei diritti dei migranti che versano in una condizione già di per sé particolarmente vulnerabile.

Mutatis mutandis, un ordine analogo di considerazioni è stato svolto con riferimento alle esenzioni relative all'impiego di sistemi di riconoscimento delle emozioni e ai sistemi di categorizzazione biometrica nel settore delle attività di contrasto previste, rispettivamente, dalle lett. f) e g) del par. 1 dell'art. 5.

Quanto al primo divieto, è chiaro, anche da quanto indicato dalla Commissione europea nelle sue linee guida del 4 febbraio 2025, l'esclusione del settore dei controlli alle frontiere e della gestione dei flussi migratori dal campo di applicazione del divieto; il che appare sorprendente se si considerano i timori manifestati dallo stesso legislatore europeo in merito all'accuratezza, all'affidabilità e ai possibili effetti discriminatori cui le *emotion recognition technologies* possono dar vita, soprattutto in un contesto come quello dei controlli degli attraversamenti dei confini dell'Unione. Senza considerare, peraltro, che trattandosi di sistemi basati sul trattamento di dati biometrici si pongono evidenti rischi di violazione del diritto alla protezione dei dati personali riconosciuto dall'art. 8 della Carta dei diritti fondamentali.

Un simile rischio si rinviene anche con riferimento all'esenzione prevista dalla successiva lett. g) che esclude dall'alveo del divieto i sistemi di etichettatura e filtraggio dei dati biometrici impiegati nell'ambito delle attività di contrasto.

Tuttavia, l'eventuale ricorso a sistemi che attuano un trattamento automatizzato di questa categoria particolare di dati personali, anche se giustificato da sopravvenute esigenze di sicurezza, dovrebbe pur sempre avvenire nel rispetto delle necessarie garanzie a tutela dei diritti in gioco e, quindi, in conformità con il diritto vigente dell'UE in materia di protezione dei dati personali.

È chiaro, quindi, che seppur in linea teorica le pratiche cui fa riferimento l'art. 5 sono considerate «inaccettabili», classificazioni errate ed eccezioni all'applicazione del divieto in parola danno vita ad un approccio differenziato e volto, ancora una volta, alla securitizzazione nei confronti di migranti.

Ciò che si auspica è, da un lato, che la Commissione europea effettui quanto prima il riesame dell'elenco delle pratiche indicate nell'art. 5, come previsto dall'art. 112, par. 1 del regolamento e, qualora necessario, che presenti opportune proposte di modifica tenendo conto degli sviluppi tecnologici e dell'effetto dei sistemi di IA sui diritti fondamentali (par. 10), inclusi quelli dei migranti oggetto di controlli da parte delle autorità di

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

frontiera, col supporto dell'Ufficio per l'IA¹²⁸ al fine di includere nuovi sistemi nell'elenco delle pratiche vietate (par. 11, lett. b)); dall'altro, che l'intervento da parte delle Corti europee contribuisca a far luce sul preoccupante impatto che questi sistemi hanno sugli individui, in particolare se in condizione di vulnerabilità come nel caso dei migranti, imponendo un innalzamento del livello di protezione dei diritti a rischio di violazione rispetto a quello che, a nostro avviso, il regolamento (UE) 2024/1389 offre.

¹²⁸ L'Ufficio per l'IA è stato istituito con decisione della Commissione, del 24 gennaio 2024, C(2024) 390, e ha il compito di sviluppare competenze e capacità dell'Unione nel settore dell'IA e di contribuire all'attuazione del diritto dell'Unione in materia di IA.

Francesca Di Gianni
*AI ACT, pratiche vietate e controlli
alle frontiere esterne dell'Unione europea*

ABSTRACT: The use of artificial intelligence systems is now a key component of European migration policy, and Fortress Europe is increasingly relying on the most innovative digital technologies for border control procedures. Regulation (EU) 2024/1689 on artificial intelligence (AI) prohibits the use of such systems, including in the context of migration governance and border controls. Article 5 of Regulation (EU) 2024/1689 prohibits the introduction, commissioning, and use of certain practices deemed «unacceptable» because they are contrary, *inter alia*, to EU values and fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union. However, the regulation provides for certain exemptions from the use of these systems, which apply specifically to external border controls. This article provides an analysis of the practices prohibited under Article 5. 5 of the AI Act that are most relevant in the context under consideration and, in particular, the problems arising from the regime of exceptions to the fundamental rights of migrants to which the law gives rise by virtue of the failure to exclude from the scope of the ban certain AI systems that are increasingly used in the sector under consideration.

KEYWORDS: AI Act – border control – migration – biometric data – prohibited AI practices

Francesca Di Gianni – Assegnista di ricerca in Diritto dell'Unione europea, Università degli studi di Bari Aldo Moro (francesca.digianni@uniba.it)