

INDICE

	<i>pag.</i>
<i>Presentazione</i> di DANIELA MILANI	XIII
<i>Le autrici e gli autori</i>	XV

RELAZIONI INTRODUTTIVE

GIUSTIZIA DIGITALE E INTELLIGENZA ARTIFICIALE: IL PROGETTO <i>NEXT GENERATION UPP</i>	3
di SILVANA CASTANO	

1. Introduzione	3
2. Il progetto <i>Next Generation UPP</i>	5
3. Il <i>Document Builder</i>	7
3.1. Architettura del <i>Document Builder</i>	9
3.2. Applicazione a un caso di studio	12

UNA LETTURA DELL'ARTIFICIAL INTELLIGENCE ACT: NORME, ETICA, ADEMPIMENTI, ATTUAZIONE	15
di GIOVANNI ZICCARDI	

1. L'avvento dell'Artificial Intelligence Act	15
2. L'incorporazione dei principi di computer ethics nell'AI Act	20
3. Un esempio pratico di carta per la governance dell'AI: il Decalogo della Statale	25
4. Gli adempimenti previsti e le concrete difficoltà	27
5. Alcune conclusioni: i limiti dei tempi di attuazione e l'attuale situazione geo-politica	30

INTELLIGENZA ARTIFICIALE E GIUSTIZIA PENALE

INTELLIGENZA ARTIFICIALE E CRISI DEL DIRITTO PENALE D'EVENTO: PROFILI DI RESPONSABILITÀ PENALE DEL PRODUTTORE DI SISTEMI DI I.A.

37

di BEATRICE FRAGASSO

1. L'intelligenza artificiale, a metà via tra *res cogitans* e *res extensa* 37
2. L'approccio europeo all'imprevedibilità algoritmica, tra normativa sulla sicurezza e modelli di responsabilità oggettiva per il produttore 44
3. Sistema di i.a. conforme alla normativa sulla sicurezza: l'efficacia esimente del rischio consentito in materia penale 47
4. Sistema di i.a. difforme rispetto alla normativa sulla sicurezza: quale spazio per l'imputazione dell'evento lesivo imprevedibile? 51
5. Dal disvalore di evento al disvalore di azione? Sulla negligente gestione del rischio da intelligenza artificiale 55

INTELLIGENZA ARTIFICIALE E INVESTIGAZIONE PENALE PREDITTIVA

61

di LUCIO CAMALDO

1. L'intelligenza artificiale nell'attività investigativa predittiva 61
2. I sistemi di polizia predittiva basati sulla localizzazione dei reati 64
3. Gli strumenti tecnologici fondati sulle serialità criminali individuali 67
4. Le questioni problematiche della *predictive policing* e la regolamentazione normativa 70
5. L'identificazione biometrica e i programmi di riconoscimento facciale 76
6. Il sistema automatico di riconoscimento delle immagini: alcuni rilievi critici 79

L'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE NELLA FORMAZIONE DELLA DECISIONE PENALE

85

di LETIZIA MANTOVANI

1. Giustizia penale e predizione algoritmica: cenni introduttivi 85

pag.

2.	Predittività della decisione: verso un diritto penale certo e calcolabile?	89
3.	La funzione aletica del processo penale messa alla prova dall'intelligenza artificiale	92
4.	I potenziali vantaggi della (parziale) automazione decisoria: le euristiche del giudice	96
5.	L'effetto <i>black box</i> e la neutralità (solo) presunta dell'intelligenza artificiale: i limiti della decisione algoritmica	100

INTELLIGENZA ARTIFICIALE E SISTEMA PENITENZIARIO 103

di GAIA CANESCHI

1.	Una premessa necessaria	103
2.	L'adeguamento tecnologico del sistema penitenziario	106
3.	L'impiego dell'intelligenza artificiale in carcere	110
3.1.	<i>Big data</i> per la verifica del superamento della c.d. ostatività penitenziaria	111
3.2.	Algoritmi predittivi della pericolosità sociale	114
3.3.	Forme avanzate di sorveglianza e controllo	119
3.4.	Nuovi elementi del trattamento rieducativo	122
4.	I prossimi passi	124

DIRITTO DELL'UNIONE EUROPEA E INTELLIGENZA ARTIFICIALE. RIFLESSI SUL PROCEDIMENTO PENALE 127

di VALENTINA VASTA

1.	Premessa	127
2.	Il cammino dell'Unione europea nella regolamentazione dell'uso dei sistemi di intelligenza artificiale	128
3.	Le regole preesistenti	132
3.1.	L'automazione nell'assunzione delle decisioni penali	133
3.2.	L'impiego di <i>software</i> che utilizzano dati biometrici	138
3.2.1.	Il riconoscimento facciale automatico	140
4.	Gli approdi dell' <i>AI Act</i> per la giustizia penale	142

	<i>pag.</i>
PROCESSO PENALE E DECISIONI ALGORITMICHE: GLI STRUMENTI DI VALUTAZIONE DEL RISCHIO	147
di ALESSIA DI DOMENICO	
1. Strumenti di <i>risk assessment</i> innovativi e prospettive d'oltre- oceano	147
2. La "giustizia attuariale" nel sistema statunitense	149
3. Costruzione dell'algoritmo e possibili spazi applicativi	150
4. Le ragioni di una crescente diffusione e le criticità dell'algo- ritmo predittivo	151
5. Alcuni recenti pronunce americane: l'opacità dell'algoritmo e la discrezionalità del giudice	152
6. Brevi conclusioni: alcuni principi-guida per un "giusto" utilizzo degli strumenti di valutazione del rischio	154
 INTELLIGENZA ARTIFICIALE E FUTURO	
 PROBLEM SOLVING CREATIVO E INTELLIGENZA ARTIFICIALE	159
di DANIELA GRIECO e GARY CHARNES	
1. Introduzione	159
2. Descrizione dell'esperimento e risultati	162
3. Il modello	165
4. Intelligenza artificiale come valutatore	167
5. Discussione e conclusioni	168
 L'INTELLIGENZA ARTIFICIALE GENERATIVA NELLA PUBBLICA AMMINISTRAZIONE	171
di RENATO RUFFINI	
 INTELLIGENZA ARTIFICIALE E DIRITTO DEL LAVORO: RISCHI (LAVORISTICI), OPPORTUNITÀ (OCCUPAZIONALI), SFIDE (REGOLATIVE)	179
di MARCO BIASI	
1. Premessa	179

	<i>pag.</i>
2. Rischi	182
3. Opportunità	186
4. Sfide	188
5. Conclusioni (aperte)	191

AUMENTARE LA SICUREZZA SUL LAVORO GRAZIE ALL'INTELLIGENZA ARTIFICIALE: LA FILOSOFIA ANTROPOCENTRICA DI INDUSTRIA 5.0 193

di CATERINA TIMELLINI

1. Introduzione al tema	193
2. L'AI Act	197
3. La tenuta del quadro normativo alla luce della tutela della salute e della sicurezza dei lavoratori	200
4. Questioni aperte e prospettive <i>de iure condendo</i>	206

INTELLIGENZA ARTIFICIALE E (IR)RESPONSABILITÀ GESTORIA: CENNI MINIMI 209

di MATTEO RESCIGNO

INTELLIGENZA ARTIFICIALE E GRUPPI DI SOCIETÀ 223

di NICCOLÒ BACCETTI

1. Introduzione	223
2. L'intelligenza artificiale quale strumento di gestione e controllo a servizio della direzione e coordinamento	224
3. Società controllate a guida autonoma	228
4. Patrimoni destinati algoritmici. Il problema dell'individuazione dei presupposti richiesti dall'ordinamento per l'esercizio di attività imprenditoriali in regime di responsabilità limitata	232

IA E TECNOLOGIE INFORMATICHE NELL'ATTUAZIONE DEI TRIBUTI: RIFLESSIONI A MARGINE DI UN DIBATTITO APPENA INIZIATO 237

di MARCO FASOLA

1. Opportunità e problemi connessi all'IA e al progresso tecnologico	237
--	-----

	<i>pag.</i>
2. Il fisco analogico: l'originaria centralità dei procedimenti di controllo e degli atti autoritativi	239
3. Il fisco digitale: acquisizione delle informazioni tramite obblighi di <i>reporting</i> e strumenti della <i>tax compliance</i>	242
4. Tre possibili strade	245

INTELLIGENZA ARTIFICIALE E DIRITTO

LIBERTÀ RELIGIOSA E AI: POTENZIALITÀ E RISCHI NELLA SOCIETÀ DELL'ALGORITMO	251
---	-----

di CRISTIANA CIANITTO

1. Libertà religiosa e AI: per tracciare un perimetro	251
2. La dimensione collettiva	254
3. La dimensione individuale	257
4. Un piccolo esperimento	259
5. Diritti fondamentali: ultima frontiera (?)	262

INTELLIGENZA ARTIFICIALE E DISCRIMINAZIONE ASSICURATIVA IN GIAPPONE	265
--	-----

di DAVIDE LUIGI TOTARO

1. Intelligenza artificiale e industria assicurativa giapponese	265
2. Contratto di assicurazione e discriminazione statistica	268
3. Promesse e limitazioni tecniche dell'uso dei sistemi di intelligenza artificiale in assicurazione	269
3.1. Il problema della causalità e del contesto	271
3.2. Il problema della opacità e imprevedibilità (effetto <i>black box</i>)	272
3.3. Il problema dei <i>bias</i> dell'algoritmo e della discriminazione	273
4. Discriminazione algoritmica e premesse della discriminazione statistica in assicurazione	276
5. Discriminazione algoritmica nel diritto giapponese	277
5.1. Parità di trattamento dell'assicurato <i>ex</i> articolo 5(1) dell' <i>Insurance Business Act</i> del 1995	277

	<i>pag.</i>
5.2. Clausole generali e principio di buona fede <i>ex</i> articolo 1 del Codice Civile	280
5.3. Discriminazione algoritmica negli strumenti di <i>Soft Law</i>	282
6. Conclusioni	285

DIRITTO DELL'UNIONE EUROPEA E INTELLIGENZA ARTIFICIALE. RIFLESSI SUL PROCEDIMENTO PENALE*

di VALENTINA VASTA

SOMMARIO: 1. Premessa. – 2. Il cammino dell'Unione europea nella regolamentazione dell'uso dei sistemi di intelligenza artificiale. – 3. Le regole preesistenti. – 3.1. L'automazione nell'assunzione delle decisioni penali. – 3.2. L'impiego di *software* che utilizzano dati biometrici. – 3.2.1. Il riconoscimento facciale automatico. – 4. Gli apporti dell'*AI Act* per la giustizia penale.

1. Premessa

Il diffondersi dei sistemi d'intelligenza artificiale (IA), che consentono, in sempre più numerosi ambiti della vita quotidiana, lo svolgimento di operazioni e compiti complessi in precedenza svolti dall'essere umano, ha reso necessario l'intervento del diritto in diversi settori dell'ordinamento.

Il fenomeno ha coinvolto inevitabilmente l'ambito giudiziario, con la possibilità di molteplici applicazioni dell'intelligenza artificiale anche nel procedimento penale. Qui, rispetto ai tradizionali strumenti, scientifici e tecnologici, a disposizione delle autorità giudiziarie e di polizia, l'intelligenza artificiale si impone con un carattere inedito, dato dalla capacità di effettuare previsioni probabilistiche, sulla base dell'elaborazione di dati e parametri, e di riprodurre capacità cognitive proprie dell'essere umano.

Il ricorso a sistemi di IA, oltre che per finalità preventive, nel procedimento penale, come strumento d'indagine, per scopi probatori e nel mo-

* Il presente contributo è già stato pubblicato sul fascicolo 1/2024 della *Rivista italiana di diritto e procedura penale*. Rispetto alla versione contenuta nella *Rivista*, il testo qui riportato è stato opportunamente aggiornato, tenendo in considerazione, in particolare, l'approvazione e la pubblicazione del testo definitivo del Regolamento dell'Unione europea sull'Intelligenza artificiale (Reg. 2024/1689).

mento decisionale, potrebbe consentire un più efficace esercizio della giurisdizione. Si assicurerebbero sia l'efficientamento delle operazioni di *law enforcement*, con risvolti positivi in termini di completezza e celerità delle indagini penali, sia la prevedibilità delle decisioni, con la conseguente riduzione degli errori giudiziari e della c.d. *sentencing disparity*.

L'ingresso dell'intelligenza artificiale nelle attività investigative, cognitive e decisionali della giustizia penale, però, può incidere negativamente sulle garanzie fondamentali: dal *vulnus* al principio di eguaglianza, considerando che «in effetti, l'algoritmo – per antonomasia – è antiegualeitario, perché considera alcuni fattori di rischio e non altri»¹, alla compromissione del diritto di difesa e dei principi del “giusto processo”: è evidente, infatti, che una decisione fondata – ed è così “appiattita” – sull'esito dell'algoritmo mette a rischio i principi di imparzialità e libero convincimento del giudice, nonché il diritto al ricorso contro una decisione ingiusta.

Vantaggi e opportunità dell'impiego dell'intelligenza artificiale impongono, in sostanza, «una parallela consapevolezza dei pericoli che essa dischiude in ragione della sua opacità, della parziale e crescente sottrazione al controllo umano, della possibilità di errori ed esiti discriminatori, potenzialmente lesivi dei diritti fondamentali»².

Per questo, nell'Unione europea l'elaborazione normativa in tema di intelligenza artificiale ha iniziato un cammino, che è rapidamente proseguito fino alla predisposizione di una disciplina organica che cerca un punto di equilibrio tra efficienza e tutela dei diritti fondamentali nello sviluppo e nell'utilizzazione di sistemi di IA. Peraltro, va detto che nel contesto europeo esistono già da tempo regole e principi entro i quali scorgere un impianto normativo in relazione all'impiego dell'intelligenza artificiale nel procedimento penale.

2. Il cammino dell'Unione europea nella regolamentazione dell'uso dei sistemi di intelligenza artificiale

L'Unione europea ha approvato il *Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e*

¹ V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *DisCrimen*, 15 maggio 2020, p. 12.

² C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal-Rivista di BioDiritto*, 2021, n. 3, p. 416.

*modifica alcune leggi dell'Unione*³, c.d. *AI Act*, al termine di un percorso costellato da diverse iniziative delle istituzioni europee finalizzate a predisporre forme di *governance* dell'intelligenza artificiale, strumentali a uno sviluppo del settore in conformità ai valori consolidati nell'ordinamento europeo.

La Commissione, dapprima con la pubblicazione delle *Draft Ethics Guidelines for Trustworthy AI*, elaborate da un gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale⁴ e poi con il Libro bianco⁵, ha fin da subito rimarcato l'esigenza che l'intelligenza artificiale sia affidabile, etica e antropocentrica e non possa prescindere dal controllo umano.

Il Regolamento (UE) sull'intelligenza artificiale è anche il risultato di un dibattito tra le istituzioni dell'Unione europea, che ha visto la Commissione, in un primo momento, propendere per interventi di modifica e integrazione degli atti già in vigore⁶, contrapporsi al Parlamento, invece, favorevole ad adottare un nuovo atto normativo che regoli in modo generale e organico la materia dell'intelligenza artificiale⁷. Con la Proposta di Rego-

³Regolamento (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) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), in G.U.U.E., 12 luglio 2024, L 1689.

⁴The European Commission's high-level expert group on artificial intelligence, *Draft Ethics Guidelines for Trustworthy AI*, in www.ec.europa.eu; gli orientamenti del gruppo di esperti sono stati condivisi dalla Commissione con la Comunicazione *Creare fiducia nell'intelligenza artificiale antropocentrica*, 8 aprile 2019, COM(2019), 168 final, nella quale accoglie con favore l'individuazione dei sette requisiti fondamentali dell'IA: intervento e sorveglianza umani; robustezza tecnica e sicurezza; riservatezza e *governance* dei dati; trasparenza; diversità; non discriminazione ed equità; benessere sociale e ambientale; *accountability*.

⁵Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia, 19 febbraio 2020, COM(2020), 65 final.

⁶Nel Libro bianco sull'intelligenza artificiale, cit., p. 15, «la Commissione ha ritenuto che il quadro legislativo possa essere migliorato per affrontare le situazioni e i rischi individuati come derivanti dall'impiego dell'intelligenza artificiale»; anche il *position paper* dal titolo *Innovative and Trustworthy AI: two sides of the same coin*, dell'8 ottobre 2020, firmato da 14 Stati membri dell'Unione europea, critica la previsione di porre prescrizioni e adempimenti obbligatori in materia di intelligenza artificiale, suggerendo, invece, di intervenire con un regime di *soft law*, capace di assicurare così la necessaria flessibilità a una tecnologia in rapida e continua evoluzione.

⁷V. per tutte la *Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale* (2020/2016(INI)), in G.U.U.E., 23 marzo 2022, C 132/17, che invita «la Commissione a valutare se sia necessario adottare una specifica azione legislativa volta a precisare ulteriormente

lamento (UE) del 21 aprile 2021⁸ la Commissione, però, si è espressa per questa seconda soluzione, motivata dalla necessità di introdurre una disciplina uniforme che contribuisca «all’obiettivo dell’Unione di essere un leader mondiale nello sviluppo di un’intelligenza artificiale sicura, affidabile ed etica» (punto 5 delle premesse) e sia funzionale a evitare che «normative nazionali divergenti possano determinare una frammentazione del mercato interno e diminuire la certezza del diritto per gli operatori che sviluppino o utilizzino sistemi di IA» (punto 2 delle premesse).

L’Unione europea, quindi, ha scelto di operare attraverso una «legislazione rigida a carattere orizzontale»⁹, che mira a garantire lo sviluppo e il funzionamento di un mercato unico digitale e a tutelare i diritti e i valori fondamentali contro i rischi derivanti dall’uso di *software* di intelligenza artificiale.

L’originaria proposta della Commissione ha subito, poi, gli emendamenti del Parlamento, approvati il 14 giugno 2023, che però hanno lasciato immutata la logica *risk-oriented* della disciplina chiaramente mutuata dal GDPR (*General Data Protection Regulation*)¹⁰, il Regolamento generale sulla protezione dei dati¹¹.

Tale Regolamento (UE), in primo luogo, indica una serie di divieti **di utilizzo dell’intelligenza artificiale**¹², perché fonte di rischi inaccettabili

i criteri e le condizioni per lo sviluppo, l’uso e la diffusione di applicazioni e soluzioni di IA da parte delle autorità di contrasto e giudiziarie» (par. 35).

⁸ *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull’intelligenza artificiale (legge sull’intelligenza artificiale) e modifica alcuni atti legislativo dell’Unione*, 21 aprile 2021, COM(2021), 206 final.

⁹ F. DONATI, *Diritti fondamentali e algoritmi nella proposta di regolamento sull’intelligenza artificiale*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. I, *Diritti fondamentali, dati personali e regolazione*, Il Mulino, Bologna, 2022, p. 121.

¹⁰ *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)*, in G.U.U.E., 4 maggio 2016, L 119/1.

¹¹ Secondo L. FLORIDI, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Philosophy & Technology*, 2022, p. 218, infatti, «from an ethical perspective, the AIA inherits the same foundational approach seen in the GDPR: it is based on protecting human dignity and fundamental rights».

¹² L’elenco è stato ampliato dal Parlamento, includendo anche i sistemi di categorizzazione biometrica che utilizzano caratteristiche sensibili (ad esempio genere, razza, etnia, stato di cittadinanza, religione, orientamento politico), i sistemi di polizia predittiva (basati su profilazione, posizione o precedenti penali), i sistemi di riconoscimento delle emozioni nelle forze dell’ordine, alle frontiere, sul posto di lavoro e nelle scuole e quelli di identificazione biometrica

per la salute, la sicurezza e i diritti fondamentali della persona. In secondo luogo, prevede regole di trasparenza armonizzate e requisiti specifici e stringenti per gli utilizzi dell'intelligenza artificiale in ambiti ritenuti "ad alto rischio"¹³, che impongono valutazioni di conformità, certificazioni, obblighi di registrazione e monitoraggio del funzionamento dei relativi sistemi, nel cui ambito si innesta pure la valutazione d'impatto sui diritti fondamentali¹⁴. Solo un obbligo di segnalazione agli utenti è invece imposto per i sistemi "a rischio limitato". Nessuna cautela è invece prevista per quelli "a rischio minimo".

Per i sistemi definiti "ad alto rischio"¹⁵, la strategia dell'Unione europea è stata orientata sin da subito a spostare il presidio delle garanzie "a monte", principalmente su *deployers* e *providers*¹⁶. In ogni caso, ai sensi del Regolamento (UE), tali sistemi devono essere progettati e sviluppati in modo tale da consentire un'efficace supervisione da parte delle persone fisiche durante il loro utilizzo¹⁷. Ciò in quanto afferiscono ad attività che richie-

remota in tempo reale ed *ex post* in spazi pubblici, pur con la previsione di alcune eccezioni per le forze dell'ordine.

¹³ Il relativo elenco è riportato in un apposito allegato del Regolamento (UE): *ANNEX III*.

¹⁴ Il *Fundamental Rights Impact Assessment* (FRIA) è stato inserito dal Parlamento nella prima bozza del Regolamento (UE), all'art. 29(a), rendendolo obbligatorio per gli utilizzatori di sistemi di IA "ad alto rischio", i quali, in base ai relativi risultati, devono sviluppare piani per mitigarne eventuali impatti negativi sui diritti fondamentali e, laddove ciò non sia possibile, devono cessarne l'utilizzo, informandone i fornitori e le autorità nazionali; in tema, v. C. NOVELLI, *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in www.federalismi.it, 2024, n. 2, pp. 110-111. L'A., in primo luogo, nota come «il bilanciamento dei diritti, operazione complessa persino per i giuristi qualificati delle Corti, spingerebbe i *deployers* ad assumere consulenti esperti legali o externalizzare questa valutazione. Anche assumendo che tutto ciò abbia un costo ragionevole per i *deployers*, questi ultimi si farebbero carico in definitiva di decisioni particolarmente sensibili»; in secondo luogo, rileva la carenza di omogeneità nelle valutazioni FRIA.

¹⁵ Per un'analisi dettagliata dei sistemi "ad alto rischio" nell'ambito della Proposta di regolamento si rinvia a G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf.*, 2022, p.p. 313-320.

¹⁶ M. VEALE, F. ZUIDERVEEN BORGESIU, *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, in *Computer Law Review International*, 2021, n. 4, pp. 102-103, notano che «*the vast majority of all obligations fall on the 'provider': in short, person or body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark*».

¹⁷ L'art. 14 (*Human oversight*), il cui testo è rimasto inalterato nel corso dei negoziati, prevede infatti che «i sistemi di IA "ad alto rischio" sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente su-

dono una componente e una responsabilità tipicamente umane, non delegabili alla macchina¹⁸.

Tra i sistemi “ad alto rischio”, già la Commissione nella proposta di Regolamento (UE) aveva indicato espressamente l’opportunità di classificare «alcuni sistemi di IA destinati all’amministrazione della giustizia e ai processi democratici [...] in considerazione del loro impatto potenzialmente significativo sulla democrazia, sullo Stato di diritto, sulle libertà individuali e sul diritto a un ricorso effettivo e a un giudice imparziale». Fra questi vanno necessariamente inclusi «i sistemi di IA destinati ad assistere le autorità giudiziarie nelle attività di ricerca e interpretazione dei fatti e del diritto e nell’applicazione della legge a una serie concreta di fatti» (considerando n. 40).

In ambito penalistico, diversi sono i contesti in cui i sistemi di intelligenza artificiale possono trovare applicazione – dagli strumenti d’indagine, come i noti *software* di riconoscimento facciale, all’attività predittiva, fino alla determinazione del contenuto di una decisione giudiziaria – su cui la regolamentazione europea è destinata a impattare¹⁹.

La Proposta di Regolamento (UE) è stata oggetto di intensi negoziati tra le istituzioni europee (i c.d. triloghi) conclusisi con l’accordo provvisorio dell’8 dicembre 2023, in base al quale anche il Comitato dei Rappresentanti permanenti (Coreper) con il voto del 2 febbraio 2024 ha adottato la posizione del Consiglio dell’UE sull’*AI Act*, il quale, in seguito all’approvazione del Parlamento e al voto del Consiglio, è diventata la prima forma di regolamentazione organica dell’intelligenza artificiale a livello mondiale, con la pubblicazione in gazzetta ufficiale del 12 luglio 2024.

3. Le regole preesistenti

Le regole *ad hoc* sull’intelligenza artificiale del nuovo Regolamento (UE) andranno a integrare altri atti, sia di *soft law*, sia vincolanti, già vigenti nel

pervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso»; per un’analisi della disposizione e dei relativi profili critici si rinvia a L. ENQVIST, ‘Human oversight’ in the EU artificial intelligence act: what, when and by whom?, in *Law, Innovation and Technology*, 2023, vol. 15, n. 2, p. 508 ss.

¹⁸ C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell’Unione Europea in materia di intelligenza artificiale*, cit., p. 429, mettono in luce come la regola «dimostr[i] un apprezzabile realismo e, al contempo, lanc[i] una sfida culturale impegnativa».

¹⁹ Si rinvia nel merito al par. 4.

diritto dell'Unione europea e rilevanti ai fini dell'impiego di sistemi di IA²⁰.

In particolare, il legislatore eurounitario ha da tempo dedicato specifica attenzione al tema della tutela del diritto alla *privacy*, declinato nella Carta di Nizza nella sua duplice accezione di diritto al «rispetto della vita privata e della vita familiare» (art. 7) e alla «protezione dei dati di carattere personale» (art. 8). Infatti, nel c.d. *Pacchetto privacy* del 2016²¹ si ritrovano alcune regole fondamentali per l'utilizzo dei sistemi di intelligenza artificiale, i quali hanno come presupposto tecnico essenziale l'elaborazione dei c.d. *big data*. Nel settore della giustizia penale, di particolare rilievo è la direttiva (UE) 2016/680 (c.d. direttiva *Law enforcement*), relativa al trattamento dei dati personali da parte delle autorità competenti a fini di «prevenzione, indagine, accertamento e perseguimento dei reati».

3.1. L'automazione nell'assunzione delle decisioni penali

La questione se affidare all'intelligenza artificiale l'attività “normalmente umana” del decidere – intesa come capacità di formulare giudizi e determinare il contenuto di una decisione – assume un'importanza fondamentale se si tratta di una decisione giudiziaria, soprattutto in materia penale. La giurisdizione penale vive, infatti, di principi – si pensi alla soggezione del giudice solo alla legge, all'obbligo di motivazione dei provvedimenti, al diritto a un ricorso effettivo – che rischiano di indebolirsi fino a perdere significato in

²⁰ V. considerando 9, 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) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), cit., per cui «le norme armonizzate stabilite nel presente regolamento dovrebbero applicarsi in tutti i settori e, in linea con il nuovo quadro legislativo, non dovrebbero pregiudicare il vigente diritto dell'Unione, in particolare in materia di protezione dei dati, tutela dei consumatori, diritti fondamentali, occupazione e protezione dei lavoratori e sicurezza dei prodotti, al quale il presente regolamento è complementare».

²¹ Esso si compone: del 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), cit.; della Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in G.U.U.E., 4 maggio 2016, L 119/89; della Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, in G.U.U.E., 4 maggio 2016, L 119/132.

rapporto a una decisione automatizzata, in quanto assunta da una macchina e non dal giudice penale libero nel suo convincimento.

Ci si interroga, allora, sulla possibilità di avvalersi dell'utilizzo di *software* durante l'intero procedimento, che possano acquisire ed elaborare tutte le informazioni rilevanti per il caso concreto e, sulla base di decisioni preimpostate assunte in casi simili, giungere alla singola decisione.

In questi casi, il diritto dell'Unione europea offre una tutela inerente alla protezione dei dati personali: l'art. 11 della direttiva (UE) 2016/680 prevede il divieto di decisioni basate «unicamente su un trattamento automatizzato, compresa la profilazione, che produca[no] effetti giuridici negativi o incida[no] significativamente sull'interessato», a meno che le stesse siano autorizzate dal diritto dell'UE o dello Stato membro al quale è soggetto il titolare del trattamento e siano previste «garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento»²². Dalla disposizione, quindi, è possibile enucleare un diritto a non essere destinatari di decisioni che si basino in via esclusiva su trattamenti automatizzati, che non prevedono alcun coinvolgimento dell'essere umano nel processo decisionale²³.

Per quanto attiene all'intensità della tutela, la direttiva (UE) 2016/680, in realtà, pur replicando quanto previsto anche al di fuori della materia penale dall'art. 22 del Regolamento (UE) 2016/679, in ordine a una decisione basata unicamente su un trattamento automatizzato²⁴, pare più incisiva rispetto a quella stabilita dalla disciplina generale²⁵. I destinatari di

²² Per S. SIGNORATO, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, in Riv. dir. proc., 2019, p. 106, il divieto in questione è solo apparente; dello stesso avviso è L. PRESSACCO, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, in G. DI PAOLO, L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Editoriale scientifica, Napoli, 2022, p. 104.

²³ Si trova già esplicita menzione nel considerando n. 38 del diritto dell'interessato a «non essere oggetto di una decisione che valuta aspetti personali che lo concernono basata esclusivamente su un trattamento automatizzato».

²⁴ La disposizione, al par. 1, stabilisce che «l'interessato ha il diritto di 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»; anche in questo contesto, l'interessato gode del diritto, riconosciutogli al par. 3, «di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestarne la decisione».

²⁵ Sottolinea infatti M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in Dir. pen. cont., 29 maggio 2019, p. 16, che «la direttiva 2016/680/UE costituisce una *lex specialis* rispetto al regolamento».

una decisione automatizzata assunta per finalità di prevenzione e repressione dei reati, infatti, non possono rinunciare preventivamente al diritto a invocare il controllo umano, come invece risulterebbe consentito dalla norma del GDPR, nel caso in cui la decisione «si basi sul consenso esplicito dell'interessato» (par. 2, lett. c) ²⁶.

Il testo del primo paragrafo dell'art. 22 del Regolamento (UE) 2016/679 lo si trova, peraltro, letteralmente trasfuso nell'art. 56 del Regolamento (UE) 2017/1939 ²⁷, che riconosce all'interessato «il diritto di non essere sottoposto a una decisione dell'EPPO 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».

In relazione all'estensione applicativa del divieto, occorre intendersi sul significato da attribuire all'espressione «decisione basata unicamente su un trattamento automatizzato». Non v'è dubbio che il diritto UE vieti, al di fuori di una specifica previsione normativa – nazionale o dell'Unione – e in assenza delle garanzie previste a tutela dell'interessato, le decisioni giurisdizionali adottate solo attraverso *software* di intelligenza artificiale, senza alcun coinvolgimento dell'intelligenza umana sul risultato decisionale.

La formulazione letterale delle disposizioni sembrerebbe avallare, però, un'interpretazione più ampia del divieto, esteso anche all'assunzione di decisioni fondate unicamente su *output* di un meccanismo automatizzato, vale a dire su elementi di prova provenienti da tecnologie di intelligenza artificiale ²⁸. D'altronde, i sistemi basati su algoritmi sono estremamente varie-

²⁶ S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 101.

²⁷ Regolamento (UE) 2017/1939 del Consiglio del 12 ottobre 2017 relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO»), in G.U.U.E., 31 ottobre 2017, L 283/1.

²⁸ Sul punto, M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, cit., p. 17, propone di valutare gli elementi di prova ottenuti mediante strumenti di intelligenza artificiale alla stregua degli indizi, che necessitano di essere corroborati da altri elementi di prova. Per l'A., infatti, «accanto all'obbligo di un intervento umano andrebbe ritenuta sussistente quella che, nel lessico processualpenalistico, chiameremmo regola di valutazione»; tale interpretazione è condivisa pure da L. PRESSACCO, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, cit., p. 106, il quale, pur riconoscendovi una certa «rigidità», ritiene «plausibile affermare che tali informazioni sarebbero idonee a dimostrare la sussistenza di determinati fatti soltanto con il concorso di ulteriori elementi di prova, in grado di bilanciarne – rispettivamente – l'eccessiva genericità o specificità», che sono «caratteristiche piuttosto comuni tra gli elementi generati o raccolti mediante dispositivi di IA» (così a p. 121); v. anche K. LA REGINA, *I.A. e ragionamento giuridico: la*

gati e, a seconda dello scopo per cui sono programmati, suscettibili di differenti applicazioni, potendo pertanto impattare in maniera e misura differente sulla decisione penale. Così, l'IA con finalità analitico-computazionali – ad esempio finalizzata al calcolo della pena o dei termini di prescrizione o alla raccolta e alla catalogazione di pronunce giurisprudenziali – si affianca a quella con finalità predittiva – ad esempio in relazione alla reiterazione di un reato o alla pericolosità sociale – che elabora dati reali per formulare una risposta in termini probabilistici, «cioè una decisione dal punto di vista logico-cognitivo»²⁹.

In sostanza, può dirsi che il legislatore dell'UE escluda la possibilità di una «delega totale all'automazione»³⁰ nell'assunzione delle decisioni giudiziarie in materia penale³¹, e richieda il controllo umano *ex post* sulle valutazioni emesse dai sistemi di IA, così da mantenere la necessaria interazione tra macchina ed essere umano (c.d. “*human in the loop*”)³².

In altri termini, come emerge dalle *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, «se un essere umano riesamina il risultato del processo automatizzato e tiene conto di altri fattori nel prendere la decisione finale, tale decisione non sarà “basata unicamente” sul trattamento automatizzato»³³,

giustizia prevedibile, in G.M. BACCARI, P. FELICIONI (a cura di), *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Giuffrè, Milano, 2023, p. 182; secondo G. UBERTIS, *Intelligenza artificiale e giustizia predittiva*, in *Sist. pen.*, 16 ottobre 2023, p. 7, «disconoscere ciò, significherebbe trascurare che la “percezione soggettiva” è ineludibile per la comprensione delle circostanze emergenti nel processo e relative alla complessità degli elementi oggettivo e soggettivo delle fattispecie penali, mentre mancherebbe la possibilità di conformare l'esito processuale alle imprevedibili cadenze della dialettica che si svolge in sede processuale».

²⁹ V. G. PADUA, *Intelligenza artificiale e giudizio penale*, in *Proc. pen. giust.*, 2021, p. 1490.

³⁰ L'espressione è di G. LASAGNI, *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma*, in G. DI PAOLO, L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Editoriale scientifica, Napoli, 2022, p. 70.

³¹ A tal proposito si parla di «principio non esclusività»; in tema v. L. LUPARIA, *Diritto probatorio e giudizi criminali ai tempi dell'intelligenza artificiale*, in R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Giuffrè, Milano, 2022, p. 782; ugualmente, in relazione all'art. 22 GDPR, v. S. MARANELLA, *La protezione dei dati personali contro un uso distopico dell'AI*, in *op. cit.*, p. 63.

³² In termini generali, v. anche *Libro bianco sull'intelligenza artificiale*, cit., p. 23, il quale in tema di prescrizioni nell'impiego dell'intelligenza artificiale “ad alto rischio” annovera «la sorveglianza umana», che «aiuta a garantire che un sistema di IA non comprometta l'autonomia umana o provochi altri effetti negativi».

³³ *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profi-*

purché il controllo non rappresenti un puro adempimento formale, ma sia tale da poter incidere significativamente sulla decisione³⁴. Inoltre, l'art. 11 della direttiva (UE) 2016/680 sembra circoscrivere, in materia penale, il divieto di decisioni interamente automatizzate ai soli provvedimenti negativi nei confronti dell'interessato, risultando sempre legittimi se producono invece effetti favorevoli.

Sul tema, ha preso posizione il Parlamento europeo con un atto d'indirizzo politico – la risoluzione del 6 ottobre 2021 *sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*³⁵ – che, in modo radicale, ha raccomandato la previsione di un «divieto dell'uso dell'intelligenza artificiale e delle relative tecnologie per l'emanazione delle decisioni giudiziarie» (par. 16).

Secondo l'Europarlamento, infatti, «gli esseri umani che fanno affidamento unicamente sui dati, i profili e le raccomandazioni generati dalle macchine, non saranno in grado di condurre una valutazione indipendente» (par. 15); il che impone di affidare le decisioni con effetti giuridici «sempre» a un essere umano, che «possa essere ritenuto responsabile per le decisioni adottate» (par. 16).

A ben guardare, la garanzia fondamentale rappresentata dalla centralità dell'intervento umano successivo sulle decisioni automatizzate, già prevista dall'art. 11 della direttiva (UE) 2016/680, più che la possibilità di mettere in discussione il merito del risultato tecnico fornito dagli strumenti di intelligenza artificiale, assicura l'individuazione del titolare del potere di emissione della decisione, ossia il giudice. Spetta, cioè, sempre a quest'ultimo il compito di valutare il risultato statistico o predittivo dall'algoritmo, consi-

lazione ai fini del regolamento 2016/679, adottate il 3 ottobre 2017, nella versione emendata e adottata in data 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione dei dati.

³⁴ Altrimenti, afferma M. BRAKAN, *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*, in *International journal of law and information technology*, 2019, vol. 27, n. 2, p. 103, «a formalistic interpretation, involving the human only as a necessary part of procedure but ultimately leaving the decision power to the machine, would not ensure a sufficiently high level of data protection of the data subject»; in senso conforme v. anche G.N. LA DIEGA, *Against the Dehumanisation of decision-Making. Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2018, vol. 9, n. 2, p. 19.

³⁵ Risoluzione del Parlamento europeo del 6 ottobre 2021 *sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale* (2020/2016(INI)), cit.; a commento v. G. BARONE, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della Risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen.*, 2022, p. 1180.

derandone il peso dimostrativo in relazione all'oggetto del giudizio, mediante un ragionamento critico che valorizzi le specificità del caso concreto.

3.2. *L'impiego di software che utilizzano dati biometrici*

Pur di fronte alle forti potenzialità in termini di efficienza nella prevenzione e nella repressione dei reati, da tempo l'Unione europea mostra un atteggiamento restrittivo rispetto all'impiego dell'intelligenza artificiale che sfrutta dati biometrici, tra cui assume rilievo il funzionamento dei *tool* di riconoscimento facciale.

Innanzitutto, una precisa definizione di dati biometrici è contenuta all'art. 4, punto 14 del GDPR, ripresa anche da altre fonti³⁶, da intendersi quali «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»³⁷.

Trattandosi di dati particolarmente sensibili, in quanto idonei a identificare in modo univoco un individuo, l'art. 10 della direttiva (UE) 2016/680 ne assoggetta il trattamento da parte delle autorità di *law enforcement* a criteri piuttosto stringenti. Esso è «autorizzato solo se strettamente necessario»³⁸, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato

³⁶ Art. 3, par. 18, *Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE*, in G.U.U.E., 21 novembre 2018, L 295/39; art. 3, par. 14, *Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*, cit.

³⁷ L'esigenza dell'*AI Act* di coordinamento con la disciplina già in vigore riguarda anche le definizioni già contenute in altri atti dell'Unione europea; per quanto attiene alla definizione di «dati biometrici», il considerando n. 14 avverte che quella utilizzata nel Regolamento (UE) («i dati biometrici possono consentire l'autenticazione, l'identificazione o la categorizzazione delle persone fisiche e il riconoscimento delle emozioni delle persone fisiche») debba essere interpretata «alla luce di» quella fornita dal GDPR e dalle direttive di settore.

³⁸ Per CGUE, Grande Sezione, 30 gennaio 2024, C-118/22, *NG*, par. 48, l'espressione «definisce una condizione rafforzata di liceità del trattamento di tali dati e implica, segnatamente, un controllo particolarmente rigoroso del rispetto del principio della "minimizzazione dei dati", quale derivante dall'articolo 4, paragrafo 1, lettera c), della direttiva 2016/680, del quale tale requisito costituisce un'applicazione specifica a detti dati sensibili».

e soltanto: a) se autorizzato dal diritto dell'Unione o dello Stato membro; b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato».

Il trattamento, anche automatizzato di dati biometrici intesi a identificare in modo univoco una persona è consentito a Europol dall'art. 30, par. 2, del Regolamento (UE) 2016/794³⁹, come recentemente modificato dal Regolamento (UE) 2022/991⁴⁰, con la «finalità di prevenire o combattere forme di criminalità organizzata nell'ambito degli obiettivi di Europol», ma pur sempre nel rispetto dei diritti e delle libertà dell'interessato attraverso le garanzie previste dallo stesso Regolamento. Tale disposizione è stata introdotta in occasione della generale investitura conferita a Europol quale promotore dello sviluppo e della diffusione di un'intelligenza artificiale «etica, affidabile e antropocentrica, che è soggetta a solide garanzie in termini di protezione, sicurezza, trasparenza, spiegabilità e diritti» (considerando n. 49).

Non deve trascurarsi che qualunque trattamento di dati biometrici finalizzato all'identificazione univoca di una persona fisica, siccome rappresenta una compressione dell'esercizio dei diritti alla *privacy* riconosciuti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, è in ogni caso soggetto al rispetto del principio di proporzionalità previsto dall'art. 52, per cui possono essere apportate limitazioni ai diritti riconosciuti dalla Carta «solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

Il Parlamento europeo, sempre con la risoluzione del 6 ottobre 2021, ha espresso, però, forte preoccupazione rispetto all'utilizzo di tali *software*, sia per «la controversa validità scientifica della tecnologia di riconoscimento utilizzata», sia, e in special modo, perché «l'uso dei dati biometrici è correlato in senso ampio al principio di dignità umana, che è la base di tutti i diritti fondamentali garantiti dalla Carta», osservando che «l'uso dell'iden-

³⁹ Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio dell'11 maggio 2016 che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI, in G.U.U.E., 24 maggio 2016, L 135/53.

⁴⁰ Regolamento (UE) 2022/991 del Parlamento europeo e del Consiglio dell'8 giugno 2022 che modifica il regolamento (UE) 2016/794 per quanto riguarda la cooperazione di Europol con le parti private, il trattamento dei dati personali da parte di Europol a sostegno di indagini penali, e il ruolo di Europol in materia di ricerca e innovazione, in G.U.U.E., 27 giugno 2022, L 169/1.

tificazione biometrica nel contesto delle attività di contrasto e giudiziarie dovrebbe sempre essere considerato ad alto rischio» (par. 30)⁴¹.

3.2.1. *Il riconoscimento facciale automatico*

Tra le tipologie di tecniche biometriche il cui impiego, specie in ambito penale, è visto con particolare diffidenza vi sono i *software* di riconoscimento facciale automatico⁴². Dalla fotografia del volto è possibile estrarre una serie di caratteristiche – come, ad esempio, la radice del naso, il punto di attacco dei capelli sulla fronte, il punto più sporgente dello zigomo (c.d. *faceprints*) – che consentono di creare il modello elettronico (*template*) di quello specifico tratto biometrico⁴³, una sorta di “codice a barre” dell’individuo, che può essere usato con finalità identificative in diversi contesti, comprese le attività di prevenzione e perseguimento dei reati. Il risultato fornito è comunque di tipo probabilistico, in quanto il sistema compara il singolo volto con tutti gli altri disponibili in una banca dati, assegnando un valore che indica il grado di probabilità che le due immagini rappresentino la stessa persona, con la possibilità anche di riscontrare una perfetta corrispondenza.

Tale metodo, rispetto ad altri di riconoscimento biometrico, se, da un lato, ha il vantaggio di non essere invasivo per il soggetto passivo, dall’altro lato, non è da questi controllabile, tanto da poter consentire l’identificazione senza la necessità di alcun atteggiamento collaborativo. Di qui, può cogliersi l’elevata efficienza di tale tecnologia, che permette la cattura dell’immagine a distanza senza che il soggetto possa accorgersene, minata, però, da un riconosciuto margine di errore piuttosto elevato, dovuto a fattori esterni che ne influenzano la *performance* – si pensi alla distanza del soggetto dal sensore, alla qualità delle immagini o alla tipologia di luce, oltre al fatto che le stesse caratteristiche del volto sono soggette a mutamenti

⁴¹ La conclusione era stata peraltro condivisa dalla Commissione nel *Libro bianco sull’intelligenza artificiale*, cit., p. 20.

⁴² A tale riguardo, basta ricordare come in un caso in materia di passaporto biometrico CGUE, Sez. IV, 17 ottobre 2013, C-291/12, *Micheal Schwarz*, par. 48, abbia riconosciuto come, laddove venga raccolta l’immagine facciale, la fotografia del volto possa provocare imbarazzo fisico e psichico per l’interessato.

⁴³ Così E. SACCHETTO, *Brevi riflessioni sui fondamenti e limiti del rapporto fra automated faced-based human recognition technology e procedimento penale*, in A. PAJNO, F. DONATI, A. PERUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. II, *Amministrazione, responsabilità, giurisdizione*, Il Mulino, Bologna, 2022, p. 541 ss., cui si rinvia per una sintetica ed efficace spiegazione del funzionamento del riconoscimento facciale tramite *software*.

– o anche alla presenza di veri e propri *bias* nello sviluppo dell'algoritmo dovuti alla qualità dei dati con cui si alimenta, con il serio rischio che il *software* possa prestarsi a controlli discriminatori e oppressivi da parte delle autorità pubbliche⁴⁴.

L'elevata probabilità di riconoscere falsamente un determinato soggetto, anche legata a pregiudizi che influenzano la progettazione dell'algoritmo⁴⁵, fa sì che l'impiego dei programmi di riconoscimento facciale – e di identificazione biometrica in generale – possa creare frizioni con la presunzione d'innocenza (art. 48 della Carta dei diritti fondamentali dell'Unione europea)⁴⁶, tanto nelle attività di polizia predittiva finalizzate a prevedere il momento e il luogo di commissione di un reato (c.d. *hotspots*) o il suo potenziale autore, quanto in fase investigativa nelle operazioni di identificazione dei responsabili di un reato già commesso.

Non stupisce, allora, che la regolamentazione di tale tecnica di controllo sia stata controversa nonché, come si dirà, oggetto di ripensamenti nel corso della stesura dell'*AI Act*.

Le istituzioni europee, tuttavia, anche al di fuori dell'*iter* legislativo dell'*hard law* avevano già assunto una linea tesa a porre un freno all'uso dei *software* di riconoscimento facciale nelle attività di contrasto. Tra queste, l'Agenzia europea per i diritti fondamentali (FRA) ha ritenuto opportuno che l'uso nelle attività di polizia sia «*strictly determined*» e limitato, oltre

⁴⁴ Tale aspetto è stato messo in luce anche dal documento della *European Union Agency for Fundamental Rights* (FRA), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, p. 27, consultabile in www.fra.europa.eu, per cui «*an important cause of discrimination is the quality of data used to develop algorithms and software. [...] Yet to date, facial images used to develop algorithms in the Western world often over-represent white men, with lower numbers of women and/or individuals of other ethnic backgrounds. As a result, facial recognition systems worked well for white men, but not for black women*».

⁴⁵ Secondo uno studio condotto dal *National Institute of Standards and Technology* degli Stati Uniti, l'utilizzo di molti *software* di riconoscimento facciale riporta molti più errori di identificazione nei confronti delle persone afroamericane, soprattutto se donne, e asiatiche rispetto alle persone caucasiche (v. P. GROTH, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FVRT). Part 3: Demographic Effects*, in www.nvlpubs.nist.gov); su tale studio e in generale sul tema v. J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in G. DI PAOLO, L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Editoriale scientifica, Napoli, 2022, p. 20 ss., il quale spiega che all'origine di tali discriminazioni vi sia «il pericolo che i creatori degli algoritmi, non selezionando in modo sufficientemente attento i volti con cui “allenare” gli applicativi, finiscano per “trasmettere” al sistema pregiudizi umani».

⁴⁶ G. BARONE, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della Risoluzione del Parlamento europeo del 6 ottobre 2021*, cit., p. 1188.

che all'identificazione delle persone scomparse e delle vittime di reato, compresi i bambini, alla lotta al terrorismo e altri gravi reati, ricalcando gli ormai consolidati limiti previsti per l'accesso delle forze dell'ordine ai *database* dell'UE su larga scala⁴⁷.

Un approccio ancora più rigido è quello adottato dal Parlamento, che, con la più volte richiamata risoluzione del 2021, ha chiesto una moratoria dell'impiego degli strumenti di riconoscimento facciale nelle attività di contrasto, «finché le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali, i risultati ottenuti siano privi di distorsioni e non discriminatori, il quadro giuridico fornisca salvaguardie rigorose contro l'utilizzo improprio e un attento controllo democratico e adeguata vigilanza, e vi sia la prova empirica della necessità e proporzionalità della diffusione di tali tecnologie»; a esclusione dei casi in cui tali strumenti siano usati per l'identificazione delle vittime (par. 27).

4. *Gli approdi dell'AI Act per la giustizia penale*

Rispetto ai profili fino a ora analizzati e ferme le disposizioni del GDPR e della direttiva (UE) 2016/680, il Regolamento (UE) sull'intelligenza artificiale è destinato a incidere con livelli di intensità diversa.

L'*AI Act* ha ampliato il catalogo degli usi vietati dei sistemi di intelligenza artificiale, in quanto portatori di un livello di rischio "inaccettabile", in ragione della potenziale violazione di diritti fondamentali, ricomprendendo, fra l'altro, lo *scraping* non mirato di immagini da internet o da telecamere a circuito chiuso per creare o espandere *database* di riconoscimento facciale (art. 5, par. 1, lett. e), i sistemi di categorizzazione biometrica che utilizzano caratteristiche sensibili, come la razza, le opinioni politiche, le convinzioni religiose o filosofiche o l'orientamento sessuale (art. 5, par. 1, lett. g) o il c.d. *social scoring* (art. 5, par. 1, lett. c).

Rimane vietata la polizia predittiva mediante l'uso di sistemi di intelligenza artificiale per effettuare valutazioni sul rischio di commissione di un reato o di recidiva di una persona fisica o di un gruppo, sulla base della profilazione o della valutazione dei tratti e delle caratteristiche della personalità (art. 5.1, par. 1, lett. d). In questo caso, il rischio che l'Unione europea ha ritenuto "inaccettabile" è la lesione della presunzione d'innocenza,

⁴⁷ European Union Agency for Fundamental Rights (FRA), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., p. 25.

per la quale le persone fisiche nell'UE dovrebbero essere sempre giudicate in base al fatto commesso (considerando 42).

Di gran rilievo nell'ambito della prevenzione e del contrasto al crimine è, inoltre, il divieto di sistemi di identificazione biometrica remota *real-time* in spazi accessibili al pubblico. Tuttavia, l'originario divieto totale da parte del Parlamento è stato temperato, in fase di negoziazione, da un numero limitato di eccezioni, cui si accompagnano una serie di cautele di salvaguardia⁴⁸. Nel dettaglio, l'uso del sistema di IA è consentito nella misura in cui sia strettamente necessario per: *i*) la ricerca mirata di potenziali vittime specifiche di sequestro di persona, tratta di essere umani, sfruttamento della prostituzione, nonché di persone scomparse; *ii*) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone o di una reale minaccia attuale o potenziale di attacco terroristico; *iii*) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, al fine di indagarlo, processarlo o sottoporlo all'esecuzione della pena di specifici reati⁴⁹, puniti nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà personale della durata, nel massimo, di almeno quattro anni, come stabilito dalla legge di tale Stato membro (art. 5, par. 1, lett. h).

Se, da un lato, il testo normativo restringe ai casi previsti l'uso dei sistemi di identificazione biometrica in tempo reale, dall'altro lato, la formulazione letterale delle eccezioni al divieto, talora generica (v. in particolare l'eccezione di cui al punto *ii*)), presta il fianco a rischi di disomogeneità applicativa nei diversi Stati membri. È innegabile, inoltre, che tale rischio si presenti anche rispetto alla possibilità di utilizzare il sistema per la ricerca degli autori di determinati reati individuati con riferimento al limite massimo editale della pena, che muta a seconda delle legislazioni nazionali.

⁴⁸ Sulla necessità di non imporre un divieto assoluto delle *facial recognition technology*, ma di puntare piuttosto su «*certain bans, limitations, regulations and monitoring*» v. V.L. RAPOSO, *Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence*, in *International Journal of Law and Information Technology*, 2022, n. 30, p. 96.

⁴⁹ L'elenco è riportato all'allegato II-Elenco dei reati di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto iii): «terrorismo, tratta di esseri umani, sfruttamento sessuale di minori e pornografia minorile, traffico illecito di stupefacenti o sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, omicidio volontario, lesioni gravi, traffico illecito di organi e tessuti umani, traffico illecito di materie nucleari e radioattive, sequestro, detenzione illegale e presa di ostaggi, reati che rientrano nella competenza giurisdizionale della Corte penale internazionale, illecita cattura di aeromobile o nave, violenza sessuale, reato ambientale, rapina organizzata o a mano armata, sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra».

L'utilizzo da parte delle forze dell'ordine dei sistemi di identificazione biometrica remota in tempo reale richiede comunque l'autorizzazione preventiva dell'autorità giudiziaria o di un'autorità amministrativa indipendente dello Stato membro, fatta salva, in casi di urgenza, la possibilità di una convalida *ex post* entro le ventiquattro ore successive all'uso del sistema, dovendosi, in mancanza, procedere immediatamente all'eliminazione e alla cancellazione di dati e risultati (art. 5, par. 3). L'attività, però, può essere autorizzata dall'autorità competente solo all'esito di un positivo vaglio di necessità e proporzionalità dell'uso del sistema di identificazione biometrica per il conseguimento di uno degli obiettivi per cui è consentita dal Regolamento e solo se l'autorità di polizia abbia eseguito il *Fundamental Rights Impact Assessment* (FRIA) (art. 5, par. 2)⁵⁰.

È possibile, invece, il ricorso a sistemi di identificazione biometrica remota a posteriori, se si tratta di attività “ad alto rischio”, ma solo al fine di ricercare una persona condannata o sospettata di aver commesso un grave reato. Tale uso deve comunque essere limitato a quanto strettamente necessario per l'indagine su uno specifico reato ed è comunque soggetto all'autorizzazione dell'autorità competente, la cui decisione è vincolante e soggetta al controllo giurisdizionale, per l'uso di tale sistema, tranne quando è utilizzato per l'identificazione iniziale di un potenziale sospettato sulla base di fatti oggettivi e verificabili direttamente connessi al reato (art. 26, par. 10).

Il Regolamento (UE) ha, infine, inserito anche una regola di utilizzabilità degli *output* dei sistemi di identificazione biometrica, escludendo che possano da soli fondare una decisione che produca effetti giuridici negativi in capo a una persona (artt. 5, par. 3; 26, par. 10).

Un'ampia gamma di sistemi di IA “ad alto rischio” è autorizzata nell'ambito delle attività di prevenzione e contrasto al crimine rimanendo soggetta a una serie di requisiti e obblighi per la diffusione e l'uso all'interno dell'UE. Tuttavia, in vista del potenziale di tali strumenti in uso alle forze di polizia, è prevista una “procedura d'emergenza” che consente alle autorità di contrasto, in situazioni di urgenza, dovute a eccezionali motivi di ordine pubblico o di specifico, concreto e imminente pericolo per la vita o l'integrità fisica delle persone, di utilizzare un sistema di intelligenza artificiale “ad alto rischio” che non abbia superato la procedura di valutazione della conformità (art. 46, par. 2).

Diversamente, l'*AI Act* non sembra aver recepito l'invito del Parlamen-

⁵⁰ Si rinvia a nt. 14.

to a vietare l'impiego di sistemi di IA finalizzato all'emissione di decisioni giurisdizionali in materia penale⁵¹.

Nell'ambito dell'amministrazione della giustizia, sono infatti classificati "ad alto rischio" i sistemi di intelligenza artificiale destinati a essere utilizzati da un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto, nonché nell'applicazione della legge a casi simili (allegato III, par. 8, lett. a). Rientra in tale categoria l'impiego di metodi computazionali nell'ambito delle decisioni penali, che rimane così assoggettato al solo controllo di conformità affidato alle stesse aziende sviluppatrici⁵².

Alla normativa dell'Unione europea sull'intelligenza artificiale, pur a fronte del frammentario e incompleto sviluppo, può di sicuro riconoscersi un primo apprezzabile risultato: il riconoscimento dell'imprescindibilità dell'intervento umano, che mantenendo il controllo sull'algoritmo, consente l'utilizzo di un nuovo metodo sinergico uomo-macchina idoneo a incrementare efficienza e qualità delle decisioni giurisdizionali.

⁵¹ Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale, cit., sulla quale si rinvia al par. 3.1.

⁵² Per S.F. SCHWEMER, L. TOMADA, T. PASINI, *Legal AI Systems in the EU's proposed Artificial Intelligence Act*, in *Proceedings of the Second International Workshop on AI and Intelligent Assistance for Legal Professionals in the Digital Workplace*, 2021, LegalAIIA, «it is noteworthy that the proposal does not follow a rights-based approach, which would, e.g., introduce new rights for individuals that are subject to decisions made by AI systems. Instead, it focuses on regulating providers and users of AI systems in a product regulation-akin manner».

