RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0280 • articolo sottoposto a peer review • pubblicato in anteprima il 7 lug. 2026

Rosa Maria Vadalà

Ricadute sostanziali delle prescrizioni e dei divieti del regolamento europeo sull'intelligenza artificiale

Muovendo da una prospettiva reo-centrica orientata ai diritti, saranno analizzate le norme dell'*AI Act* che incidono sull'azione penale, evidenziandone le potenzialità garantistiche, sostanziali e processuali. Tali potenzialità si confrontano, da un lato, con la legge italiana sull'intelligenza artificiale (l. n. 132/2025), che non ha sostanzialmente introdotto istituti idonei a recepire nel processo penale le previsioni sovranazionali; dall'altro, con le disposizioni penali nazionali che incidono sull'operatività dell'*AI Act*. Costituisce inoltre un limite invalicabile il sistema di divieti ed eccezioni delineato dall'art. 5 del regolamento europeo, che si fonda sul diritto all'autodeterminazione informativa e sul principio di proporzionalità. Quest'ultimo consente quella capacità di resistenza dei diritti rispetto a derive securitarie, per cui l'AI potrebbe segnare un punto di non ritorno.

Intelligenza artificiale – Giustizia penale – Proporzionalità – Reo – Diritti fondamentali

Criminal implications of the prohibitions and restrictions of AI ACT

Adopting a defendant-centred, rights-based perspective, this article examines the provisions of the AI Act that affect criminal proceedings, highlighting their substantive and procedural safeguards. The effectiveness of these safeguards must be assessed, on the one hand, in light of the Italian Artificial Intelligence Act (Law No. 132/2025), which has largely failed to introduce legal mechanisms capable of incorporating the supranational framework into criminal proceedings, and, on the other hand, against the backdrop of domestic criminal law provisions that shape the implementation of the AI Act. A further, non-derogable constraint is represented by the system of prohibitions and exceptions established under Article 5 of the Regulation, which is grounded in the right to informational self-determination and the principle of proportionality. The latter provides a crucial safeguard against security-driven excesses, in the face of which AI could otherwise mark a point of no return.

Artificial intelligence – Criminal justice – Proportionality – Offender – Fundamental rights

L'Autrice è docente a contratto di Cybercrime presso il Dipartimento di informatica dell'Università di Verona

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2,* a cura di Gaetana Morgante e Gaia Fiorinelli

1. Premessa sulla dimensione sostanziale in gioco

L'analisi delle ricadute sostanziali delle previsioni del regolamento (UE) 2024/1689, c.d. *AI Act*, sugli impieghi di sistemi intelligenti in funzione di prevenzione e accertamento dei reati[1] chiama in causa la più ampia riflessione sui diritti fondamentali in gioco. Come messo chiaramente in luce, l'atto regolamentare esplicita quel "nesso molto significativo tra l'ambizione alla sovranità digitale da parte dell'Unione europea e la stessa identità costituzionale europea, laddove la prima risulta funzionale al consolidamento di quel costituzionalismo digitale europeo (…) in modo che quest'ultimo possa disporre dei poteri adeguati a garantire la tutela dei diritti fondamentali"[2].

Per la giustizia penale l'adozione di questa prospettiva concentra il focus d'intervento della legge sulla sfera giuridica dell'individuo sulla quale lo *ius puniendi* sarà destinato a dispiegarsi. Come è stato autorevolmente evidenziato, "il contributo più significativo offerto dalla giurisprudenza di Strasburgo (…) è quello di avere chiarito che ogni estrinsecazione di potere pubblico abbisogna di una giustificazione dalla specifica prospettiva della persona sulla quale il potere va ad incidere, chiamando necessariamente in causa i suoi 'diritti' di fronte all'autorità"[3].

In particolare, lo sviluppo tecnologico consente indagini pro-attive, che combinano aspetti di quelle preventive e di quelle repressive[4], configurandosi come attività esplorative volte alla ricerca delle notizie di reato[5]. Questa commistione si traduce nell'impiego di "tecniche operative miste, anfibie, ambivalenti"[6] con una crescita non solo dei poteri e compiti di polizia, ma anche della commistione con le attività di *intelligence*[7]. Quanto sopra impone di anticipare la predetta visione "orientata" ai diritti ad una fase antecedente al processo o al procedimento penale[8], estendendo l'ambito da presidiare agli atti particolarmente intrusivi di tipo investigativo in senso ampio.

1. Riconoscono ante *AI Act* le potenzialità dell'AI in questa duplice direzione Borges Blàzquez 2021, p. 111; Manes 2020, p. 6.
2. Caramaschi 2025, p. 10.
3. Viganò 2023, p. 17.
4. Signorato 2016, p. 194; Blount 2021, p. 39.
5. Torre 2019, p. 1437.
6. Negri 2016, p. 3.
7. Nocerino 2020, p. 822.
8. Sulla prospettiva del diritto penale reo centrico, che concepisce il soggetto nei confronti del quale si procede come l'anello debole della macchina repressiva si rinvia, anche per i relativi riferimenti bibliografici, a Bernasconi 2022.

In conformità, pertanto, sia alle peculiarità dell'intelligenza artificiale, quale tecnologia di per sé *disruptive*[9], sia alla sua idoneità ad operare più come strumento d'indagine, che di giudizio[10], l'*AI Act* considera quale contesto "penale" di riferimento quello di *law enforcement*, quale "attività svolta 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"[11].

Questa scelta di campo è espressione emblematica di un tecno-diritto[12], che non è più declinabile secondo una prospettiva di prevalenza o di resistenza della legga rispetto al *code*[13], ma d'integrazione funzionale, che, alla luce dei nuovi fattori di rischio tecnologico, estende o introduce apposite garanzie sostanziali e procedurali, consentendo, però, quegli impieghi di sistemi di AI che possono apportare importanti benefici.

Per evitare, però, che la trasformazione tecnologica alimenti un'inammissibile diritto penale *gendarmo*[14], che sublima prevenzione e sicurezza, queste garanzie dovrebbero essere funzionali a confinare entro un'area di *legal risk*[15] le potenzialità pregiudizievoli associabili a questi impieghi.

Il richiamo al concetto di rischio non è qui, però, operato secondo quella logica di tipo precauzionale di cui certamente è pervasa l'*AI Act*, data la classificazione delle forme di manifestazione dell'intelligenza artificiale a cui si associano regimi differenti[16]. Come autorevolmente evidenziato, gli standard richiesti dal regolamento europeo costituiscono la futura piattaforma concettuale per la disciplina dei profili di responsabilità penale per l'immissione nel mercato e l'utilizzo di strumentazioni di AI[17].

Ma la prospettiva che qui si intende adottare è un'altra: guardare a questi standard come fattori che confinano l'invasività o potenzialità lesiva dell'AI quale strumento dell'azione di contrasto. Per essere più chiari, il *legal risk* a cui si fa riferimento dovrebbe essere la traduzione normativa di quel bilanciamento, costantemente ricercato dalle Corti per le indagini tecnologiche, tra le esigenze

9. *Disruptive innovation* è termine coniato nel 1995 da Clayton Christensen per indicare l'effetto di una nuova tecnologia o di un nuovo modo di operare su un modello di business, che porta a modificare completamente la logica fino a quel momento presente nel mercato, introducendo comportamenti e interazioni nuove. Sul punto Christensen–Raynor–McDonald 2015, p. 44 ss.
10. Camon 2025, p. 3009.
11. In questi termini l'art. 3, n. 46, dell'*AI Act*.
12. Per Amato Mangiameli 2023, p. 469 ss., questa espressione designa il diritto con/della/per la tecnologia, potendosi in proposito distinguere: 1. le procedure prodotte dall'evoluzione tecnologica e recepite dal diritto; 2. quelle sinergicamente generate dalla tecnica e dal diritto; 3. quelle sviluppate dal diritto per disciplinare la tecnica.
13. Sul rapporto tra *code* e legge Lessing 2000; Hassan–De Filippi 2017, p. 88. Con specifico riferimento al diritto penale Sgubbi 2019, p. 40, discorre di formante algoritmico per rappresentare come nel sistema penale, che si avvia ad essere disciplinato tramite codice, la certezza del tipo di fatto punito dipende dalla predittività della decisione giudiziale fondata su calcoli algoritmici.
14. Barona Vilar 2019, p. 33.
15. Per Canato 2024, p. 15, questo rischio è costituito da quella quota di rischi che residua dai presidi imposti dall'*AI Act* ed è predeterminata senza un'adeguata attenzione alla effettiva dimensione fattuale.
16. I sistemi di AI sono classificati secondo 4 livelli di rischio: inaccettabile, alto, limitato e minimo. Nel presente lavoro verranno considerarti solo i primi due livelli a cui corrispondono sistemi che, per l'impatto che possono avere sui diritti fondamentali, sono o vietati, ancorché con alcune eccezioni limitati, o ammessi, ma nel rispetto di requisiti molto rigorosi.
17. In questi termini Consulich 2024, per cui nonostante "la categorizzazione impiegata, che sostanzialmente identifica una scala decrescente di rischio, ha una conformazione statica (…) nel testo del Regolamento emerge la consapevolezza di dover adottare un modello di regolazione flessibile per adeguarsi ad un contesto fattuale così fluido: non a caso infatti, ma per necessità, si assiste all'impiego di norme standard, che non descrivono condotte vietate, ma livelli di sicurezza da soddisfare, sulla base di valutazioni tecniche".

di tutela dei diritti fondamentali e l'interesse generale all'accertamento dei reati[18].

Non è un caso che principio, attraverso cui l'*AI Act* sembra tentare di fare ciò, è quello di proporzionalità, il quale richiede di rapportare l'importanza dell'obiettivo perseguito con l'atto d'indagine alla gravità dell'ingerenza, come schermata dalla qualità e quantità delle cautele applicabili a favore dei soggetti interessati[19].

Allo stesso tempo sembra che il regolamento, almeno con riferimento ai sistemi maggiormente invasivi per i diritti, vada oltre questa impostazione[20], mostrando un'attenzione che è pregevole se pensiamo che l'*AI Act* "si rivolge al mercato e non ai soggetti istituzionali, prima istanza di presidio delle garanzie fondamentali": il regolamento va ascritto entro "una cornice dettagliata e consolidata, costituita dalla stratificazione di molti strumenti normativi specificamente legati alla dimensione 'non tecnica', ma processuale"[21].

2. L'AI nella giustizia penale: disposizioni "dirette" dal regolamento (UE) 2024/1689 alla legge n. 132/2025

Con questa consapevolezza vanno considerate le prescrizioni che in via non solo diretta, ma soprattutto indiretta impattano sull'azione penale.

In via diretta, l'allegato III, paragrafo 6, indica alcune tipologie di sistemi di AI impiegabili nell'attività di contrasto, tra cui, alla lett. a), quelli per determinare il rischio per una persona fisica di diventare vittima di reati.

Premesso che la vittima è "tradizionalmente tenuta alla porta dal magistero punitivo"[22], sia che si adotti la visuale europea, che la identifica con il soggetto direttamente o indirettamente pregiudicato dal reato, sia quella dogmatica, che guarda al titolare del bene offeso[23], il concetto di vittima rimanda oggi sempre più ad un bisogno particolare di protezione mediante il diritto penale. A fronte dell'emersione di supervittime, come minori o donne[24], e della categoria delle vittime potenziali, quali titolari del diritto fondamentale alla sicurezza[25], lo statuto penal-processuale ha finito però per assumere un'impronta paternalistica vittimocentrica, divenendo modulabile in funzione del tipo di fatto o del tipo di autore. A fronte di reati che cercano di coprire fenomeni sociali complessi, questa modulabilità dello statuto si è tradotta nella mobilità delle garanzie, innalzabili per la vittima ed abbassabili per l'autore[26].

Alla luce di quanto sopra, al fine di evitare che anche l'AI ricada in questa logica efficientista securitaria, potenzialmente in contrasto con la visione reo centrica orientata ai diritti che abbiamo avanzato nella premessa, opportuna appare la delimitazione dell'impiego dei sistemi di *victim prediction* ad alcuni reati particolarmente gravi o afferenti a dinamiche che ne compromettono l'emersione.

Sotto questo profilo, il pensiero corre immediatamente a quei *tool* che sono stati sviluppati a partire da *VioGén*, che è uno strumento algoritmico che stima il rischio di ri-vittimizzazione delle donne che hanno denunciato episodi di violenza

18. Su questo bilanciamento, alla luce della giurisprudenza della Corte di giustizia e di alcune Corti Costituzionali europee, con riferimento alla *data retention* ed alle altre indagini investigative a contenuto tecnologico, si rinvia a Flor 2022, p. 74 ss.
19. Sulla configurazione sovranazionale del principio di proporzionalità, come emergente in particolare dalle statuizioni adottate dalla Corte di giustizia con la pronuncia del 30 aprile 2024, C178/22, in tema di *data retention*, Parodi 2025, p. 11.
20. Questa valutazione è imposta per l'impiego di sistemi di riconoscimento facciale *real time*, per cui si rimanda al paragrafo 4.
21. Così Quattrocolo 2025.
22. Bernasconi 2019, p. 2.
23. Su questa duplice visione vedi Venturoli 2017.
24. Pavan 2013, p. 4 della versione digitale consultabile nella banca dati *one legale*.
25. Venturoli 2021, pp. 9-10.
26. Maggio 2017, p. 694.

domestica[27]. Risponde a finalità analoghe anche il sistema intelligente *Vides* (*Violence detection system*) elaborato da un team multidisciplinare dell'Università di Torino per rilevare episodi di violenza sulla base dell'analisi dei referti del pronto soccorso[28]. In linea con la trasparenza che l'*AI Act* impone quale requisito dei sistemi ad alto rischio, *Vides* è stato progettato in modo da esplicitare gli elementi che supportano l'interpretazione del referto come relativo a lesioni di origine violenta[29].

A fronte anche di questa "spiegabilità", l'impiego di sistemi simili è apprezzabile dal punto di vista penale perché consente d'intercettare reati, come i maltrattamenti in famiglia, in cui la violenza è pratica reiterata in una condizione di soggezione della vittima ed in assenza di testimoni[30]. Le potenzialità dell'AI, consentendo un tempestivo rilevamento di queste dinamiche, contribuirebbero ad incrementare, ad avviso di chi scrive, il livello d'effettività ed efficacia della disciplina nazionale contro non solo la violenza domestica, ma anche di genere, prevenendo potenziali decorsi tragici, come il femminicidio[31]. Proprio alla luce dei contenuti della recente riforma che ha portato all'introduzione di questo reato[32], il regolamento in esame potrebbe essere valorizzato per colmare la mancata adozione di previsioni apposite su modi e tempi di valutazione del rischio di *escalation* da parte di operatori di polizia e giudici; in questo modo verrebbe, peraltro, dato corso ai moniti inascoltati della Corte di Strasburgo, che concepisce queste procedure di valutazione cruciali ai fini dell'adempimento degli obblighi di tutela discendenti dalla Convenzione di Istanbul[33].

Anche in considerazione di questo contributo, i sistemi di AI di *victim prediction* risultano impiegabili in maniera affidabile e senza grandi criticità essenzialmente come strumenti predittivi con compiti di screening iniziale[34]. In questo modo è evitabile il rischio, da cui abbiamo preso le mosse, di disequilibrio tra la protezione accordata alla vittima e le garanzie spettanti al reo. Sul punto, peraltro, la qualificazione ad alto rischio anche di questi sistemi ne comporta la sottoposizione a regole di *compliance* per sviluppatori e *deployer*, che possono positivamente impattare sulla posizione del reo, come gli oneri di trasparenza e robustezza, nonché di supervisione umana[35]. Per autorevole dottrina anzi alcune disposizioni del regolamento rileverebbero propriamente quali garanzie processuali aggiuntive[36]. In particolare, le prescrizioni relative sia all'iscrizione dei sistemi di AI in banche dati[37] e alla registrazione

27. Sulle caratteristiche tecniche di questo sistema e sulle sue criticità, soprattutto sul piano della compatibilità tra la logica tecnologica, basata sulla predizione del rischio individuale, e gli obiettivi del quadro legislativo spagnolo sul contrasto alla violenza di genere e alla violenza sessuale, vedi Morondo Taramundi 2025, p. 69.
28. Mensa–Colla–Dalmasso et al. 2020, p. 263 ss.
29. *Ivi*, p. 271.
30. Cass. pen., Sez. VI, 11 settembre 2025, n. 35067/2025; Cass. pen., Sez. VI, 18 aprile 2023, n. 16466.
31. Sulla configurazione del reato di maltrattamenti in famiglia quale antecedente o reato spia di questo epilogo nella sua valenza sociologica Cass. pen., Sez. I, 12 aprile 2022, n. 14016; Colone–Esposito–Meglio et al. 2023, p. 101 ss. Sul femminicidio quale fattispecie di reato sia consentito rinviare, senza alcuna pretesa di esaustività, a Massaro 2025, Pecorella 2025, Di Nicola Travaglini 2025.
32. Lazzeri 2025.
33. Pulito 2024, p. 223.
34. In senso critico Pulito 2024, p. 231, che lo concepisce come un uso depotenziato questi strumenti.
35. Norme di riferimento sul punto sono: l'art. 9 sull'adozione di un sistema di gestione dei rischi, l'art. 11 sull'aggiornamento della documentazione tecnica, l'art. 12 sulle procedure e tempi di registrazione automatica degli eventi, l'art. 13 sulla trasparenza del funzionamento, l'art. 14 sulla supervisione umana e l'art. 15 sui requisiti di accuratezza, robustezza e cybersicurezza.
36. Camon 2025, p. 3019, che ritiene in questo senso particolarmente rilevante l'art. 14 comma 5) sul principio dei "quattro occhi".
37. Ai sensi dell'art. 49 dell'*AI Act* per i sistemi ad alto rischio di cui all'allegato III, paragrafo 6, impiegati nelle attività di contrasto la registrazione avviene, però, in una sezione sicura non pubblica della banca dati dell'Ue di cui all'articolo 71 e comprende, a seconda dei casi, solo alcune informazioni.

automatica degli eventi[38] sia quelle che, a certe condizioni, consentono l'accesso ai codici sorgenti attuerebbero rispettivamente quelle istanze sulla tracciabilità della prova informatica e sull'effettività del contraddittorio sull'ammissibilità dello strumento computazionale e dei relativi output[39].

Pur condividendosi questa opinione, si ritiene che le potenzialità processual-garantistiche di queste regole richiedano uno sforzo "ricettivo" al livello nazionale, che non è stato al momento esercitato dalla legge n. 132/2025, contenete le "disposizioni e deleghe al Governo in materia di intelligenza artificiale".

Infatti, i non detti di questa legge sono superiori ai detti, essendosi limitata, da un lato, a riservare al magistrato ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti. Dall'altro, è stata conferita delega per l'adozione di disciplina apposta sugli impieghi dei sistemi di AI rispettivamente al Ministero della giustizia per l'organizzazione e semplificazione del lavoro giudiziario e al Governo per l'attività di polizia[40].

Si tratta di poche e deludenti disposizioni che nulla apportano sul piano degli istituiti e delle categorie che possano veicolare nella giustizia penale le previsioni sovranazionali. In proposito si rammenta che queste previsioni vanno in ogni caso applicate, per espressa disposizione del regolamento relativa proprio ai sistemi del predetto allegato III, conformemente al diritto nazionale.

Quanto sopra comporta che la legge n. 132/2025, così come anche le altre previsioni di contenuto specificamente penale impattino sulla operatività dell'*AI Act*, limitandola o fungendo da vero e proprio sbarramento.

Nel primo senso, la segnalata riserva decisoria al magistrato prevista dalla legge n. 132 assegna una funzione ausiliare a quei sistemi di AI di cui alla lett. c) dell'allegato III, relativi alla valutazione di affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati. Anzi, in forza del coordinamento garantistico tra fonti, dovrebbe ritenersi che la valutazione del sistema operi a supporto della decisione giudiziale in via succedanea ed a maggior ragione se a favore del prevenuto[41].

Un effetto di sbarramento in senso proprio è svolto, invece, dall'art. 188 c.p.p. con riguardo ai sistemi di cui alla lett. b) dell'allegato III, che possono svolgere funzioni di poligrafo. Il divieto nazionale di metodi o tecniche che siano idonee ad influire sulla libertà di autodeterminazione riguarda, infatti, i sistemi che generano anche solo una qualche forma di pressione, a causa dello stato di soggezione psicologica del soggetto esaminato[42]. Ulteriore rischio che il divieto nazionale sarebbe chiamato ad evitare è quello di trasformare l'individuo, attraverso il ricorso a questi sistemi, "da 'fonte di prova dichiarativa' a 'fonte di prova reale'" con compromissione della sua dignità umana[43].

Com'è stato giustamente rilevato, però, la rigidità di questo divieto non dovrebbe essere considerata assoluta almeno per il testimone, che è obbligato a dire la verità[44]; anche per il reo potrebbe ritenersi recessivo, in presenza di libero e volontario consenso[45] a sottoporsi a verifiche di verità condotte con sistemi di AI, che siano affidabili perché *complaiant* agli standard del regolamento e necessari per dimostrare la sua innocenza.

3. Profilazione tra conferme e novità

Le previsioni dell'allegato III, paragrafo 6, sui sistemi intelligenti per determinare il rischio di commissione del reato o di recidiva, e di profilazione (lett. d) ed e)) ripropongono non solo la necessità di coordinamento multilivello tra le fonti, ma

38. In base all'art. 12 dell'*AI Act* i sistemi ad alto rischio devono essere muniti di meccanismi per la registrazione automatica degli eventi ("log") per l'intera durata del ciclo di vita del sistema.
39. Camon 2025, p. 3018.
40. Art. 15 comma 2 e art. 24 lett. h) della legge n. 132/2025.
41. Non introducono sul punto preclusioni, ammettendo che le risultanze dell'AI possano supportare una decisione anche sfavorevole, Luparia–Fiorelli 2022, p. 42.
42. Chelo 2025, p. 113.
43. Luparia–Fiorelli 2022, p. 39.
44. Camon 2025, p. 3016.
45. In questi termini, con riguardo a "prove di verità" di matrice neuroscientifica, Palma 2020, pp. 56-57.

anche criticità sul piano della coerenza interna dell'*AI Act*. L'ammissibilità o meno di questi sistemi è, infatti, questione da definire in coordinamento con l'art. 5 del regolamento, che individua quelli vietati perché generativi di rischi inaccettabili[46].

Aspetto problematico di questo intreccio è che l'art. 5 definisce questi sistemi mediante "fattispecie complesse, descritte attraverso nozioni talvolta generiche e, in ogni caso, costruite attorno a una serie di limiti, espliciti o impliciti"[47].

In questo senso emblematica è proprio la lett. d) dell'art. 5 che, da un lato, in apparente contraddizione con le sopra indicate lettere d) ed e) dell'allegato III, vieta l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di AI per prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione o della valutazione dei tratti e delle caratteristiche della personalità; dall'altra, ammette, però, quei sistemi di AI utilizzati a sostegno della valutazione umana del coinvolgimento oggettivamente comprovato e verificabile di una persona in un'attività criminosa.

Il predetto divieto opera a tutela della presunzione d'innocenza[48] e del principio di materialità del diritto penale[49]. La definizione dei sistemi intelligenti predittivi e di profilazione esterni alla sua area rileva, in particolare, quale "coefficiente di resistenza" di un diritto penale del fatto, in quanto "se l'attività giurisdizionale concretizza l'ordinamento è evidente che le sue disposizioni sono le norme di chiusura dello stesso, volte ad assicurare la sua complessiva tenuta"[50].

Per poter comprendere quali sistemi di profilazione e di predizione siano ammissibili è necessario operare prima di tutto un previo distinguo tra predizione e profilazione. Partendo dalla profilazione, nonostante l'*AI Act* richiami sul punto la nozione del GDPR, riferimento specifico per il contesto penale non può che essere la direttiva (UE) 2016/680, c.d. LED, 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[51]. In attuazione dell'atto sovranazionale, il d.lgs. n. 51/2018, definisce la profilazione come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati 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 persona fisica"[52]. Sulla scia della direttiva attuata e del GDPR, il decreto vieta, inoltre, espressamente le decisioni basate unicamente su un trattamento automatizzato che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge, in presenza di garanzie adeguate per i diritti e le libertà dell'interessato. È altresì precisato che queste decisioni non possono, in ogni caso, basarsi su quelle categorie di dati personali previsti dall'art. 9 del GDPR, il cui trattamento può generare il rischio di discriminazioni[53].

Questo divieto ed in generale le misure relative ai diritti dell'interessato e sul trattamento dei dati

46. Si segnala che le disposizioni del regolamento relative a questi sistemi sono applicabili già a partire dal 2 febbraio 2025 perché, come specificato al considerando 179, "sebbene la piena efficacia di tali divieti discenda dall'istituzione della governance e dall'esecuzione del presente regolamento, è importante anticipare l'applicazione di detti divieti per tenere conto dei rischi inaccettabili e avere un effetto su altre procedure, ad esempio nel diritto civile".
47. Speziale 2025, p. 340.
48. In questo senso esplicito è il considerando 42 dell'*AI Act*.
49. Su questo principio, quale baluardo di un diritto penale di libertà, Mantovani 1992, p. 25.
50. Ruggiero 2023, p. 1485.
51. Si rinvia per un'analisi della *ratio* e dei contenuti che contraddistinguono questo atto europeo a Galgani 2019, pp. 5-8.
52. Così art. 2, lett. e, d.lgs. 51/2018; per un'analisi sul punto si rinvia a Baccari–Conti 2021, p. 711 ss.; Ziroldi 2019.
53. Si tratta dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dei dati genetici, di quelli biometrici, intesi a

in sé, quale espressione dei principi di *privacy by design* e *privacy by default*, fungono da fattori di emersione e rimozione degli eventuali pregiudizi[54].

Rispetto a questo assetto, la previsione dell'allegato III, lett. e), che ammette l'impiego dell'AI profilativa può essere concepita come "confermativa": ne bilancia l'insidiosità attraverso le apposite cautele discendenti dalla qualificazione di questi sistemi ad alto rischio, compresi i requisiti in materia di set di dati di addestramento, convalida e prova.

Allo stesso tempo, l'art. 5 non fissa alcuna preclusione in ordine alla profilazione in sé, anche se "intelligente". Conformemente alla *ratio* di questa disposizione, ad essere vietati sono i sistemi di AI di valutazione del rischio individuale di commissione di reato che si fondino esclusivamente sulla profilazione. In questo modo l'area del divieto ne include solo un utilizzo e specificamente quello che, a causa della sua valenza determinante rispetto alla predizione del rischio reato, non ci tiene indenni da un diritto penale d'autore perché "proiettando la valutazione del singolo caso sullo sfondo di generalizzazioni statistiche in funzione predittiva, allontana la valutazione dal fatto"[55].

3.1. Il divieto dell'art. 5 tra predizione "decisoria" e predizione di polizia

Stesso discorso vale per i sistemi di AI in cui questa predizione è fondata unicamente sulla valutazione dei tratti e delle caratteristiche della personalità del soggetto e non sia a supporto di un previo giudizio umano attestante, sulla scorta di elementi fattuali obiettivi, il suo coinvolgimento in attività criminosa. Come chiarito dalle linee guida emanate dalla Commissione in funzione orientativa per l'interpretazione e l'applicazione dei divieti e delle eccezioni dell'art. 5[56], la predetta ipotesi è da concepire come alternativa rispetto alla profilazione, in quanto categoria ampia a valenza residuale. Sul punto, aspetto, che è messo in luce dalla Commissione e che è idoneo ad influire sull'affidabilità e attendibilità di queste valutazioni, riguarda la distinzione, applicabile anche alla profilazione, delle caratteristiche personali in "Known, inferred or predicted": se le prime costituiscono input verificabili, le seconde e le terze o si basano su informazioni dedotte dal sistema da altri dati o sono stimate sulla base di modelli, con un grado di accuratezza inferiore al 100%[57].

Queste due ultime categorie sono proprio quelle informazioni che sarebbe più complesso e con tempi più lunghi ottenere da un'analisi manuale dei dati, con la conseguenza che essi rappresentano al tempo stesso il "valore aggiunto – ma anche il potenziale lesivo – dell'automazione"[58].

Nella dottrina nazionale, poi, la diffidenza verso sistemi che impiegano aspetti afferenti alla personalità in funzione di *risk assessment* è strettamente connessa alla loro riconduzione alla c.d. "perizia criminologica", con conseguente operatività del divieto dell'art. 220, comma 2, c.p.p., quale norma, pertanto, di sbarramento[59].

In realtà, la predetta associazione appare non convincente tanto nel merito della somiglianza dei sistemi di AI in esame con la verifica peritale, essendo l'output l'esito dell'elaborazione di dati e non certo di esplorazione del foro interiore della persona, quanto per la sua eccessiva rigidità rispetto a quell'esigenza d'individualizzazione dell'accertamento che è imposta dai diversi istituti – afferenti sia alla fase delle indagini, sia a quella del giudizio, come pure al momento dell'esecuzione

identificare in modo univoco una persona fisica, e di quelli relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

54. Pietrocarlo 2023, p. 57.

55. Manes 2020, p. 13.

56. Si tratta delle *Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, doc. C (2025) 5052, che costituiscono, come esplicitato da Speziale 2025, p. 345, uno strumento di soft law privo di efficacia vincolante.

57. In proposito il paragrafo 4.2.1. delle *Guidelines*.

58. Merler 2023, p. 688.

59. Macrì 2025, p. 11 ss.

della pena – che impongono, ancorché in misura diversa, un giudizio personologico[60].

I sistemi predittivi sono idonei a soddisfare le esigenze valutative imposte da queste differenti fasi, essendo distinguibili in quelli: (1) *pre-crime*[61], che sono impiegabili nella gestione della sicurezza pubblica e specificamente nella attività di polizia[62] per fare previsioni su futuri eventi criminali; (2) *pre-trial*, che consentono la prognosi di pericolosità per l'applicazione di misure cautelari custodiali; e, infine, (3) di *sentincing*, che sono utilizzabili per la commisurazione della pena e la valutazione del rischio recidiva[63].

L'allegato III, paragrafo 6, sembra riferibile sulla base della formulazione testuale ai sistemi di *pre-trial* e di *sentencing*. Questa conclusione è confermata dalle linee guida della Commissione, che ne delimitano l'operatività, in conformità all'art. 5, in funzione di ausilio della decisione dell'autorità competente che si basi già su fatti oggettivi e verificabili, direttamente connessi a un'attività criminosa[64].

Tale funzione di ausilio deve comunque fare i conti, in particolare per i sistemi AI di *sentencing*, con la necessità di adottare misure sanzionatorie che siano idonee a "perseguire quei risultati di individualizzazione e di risocializzazione fissati dalla Costituzione", superando quella "concezione processuale tuttora saldamente ancorata ad una giustificazione retributiva della pena e ad anacronistici retaggi del tecnicismo giuridico"[65].

Ma la predizione intelligente con cui siamo chiamati a confrontarci ha carattere eminentemente probabilistico, operando secondo regole di tipo essenzialmente statistico e di natura criminologica[66], con la conseguenza che l'auspicata individualizzazione può essere supportata dall'impiego di questi *tool* solo laddove l'output, che sia ottenuto anche mediante elaborazione di dati personalistici, venga calato nella specificità del caso concreto.

Ritornando alla predetta decisione umana oggettivamente fondata e verificabile, con cui le risultanze intelligenti saranno chiamate ad integrarsi in via subalterna, interessante è il tentativo delle linee guida della Commissione di definirla alla luce delle statuizioni adottate dalla Corte di giustizia in ordine al divieto di decisioni completamente automatizzate sul rischio che i passeggeri

60. Come chiarito da Pulito 2025, p. 16, la valutazione della personalità dell'imputato rileva: nella fase delle indagini per l'applicazione delle misure cautelari; nel giudizio per la commisurazione della pena o per l'applicazione delle misure di sicurezza; nella fase dell'esecuzione della pena per una concreta determinazione del trattamento penale.

61. Giraldi 2020, p. 47.

62. Sorbello 2019, p. 377, definisce la polizia di sicurezza come quelle "varie attività finalizzate al riscontro e alla ricerca di situazioni 'oggettive' di pericolo o di inizio di attività criminose (…) Essa ha carattere preventivo in quanto è tesa ad impedire qualunque violazione dell'ordine sociale e si differenzia dalla polizia giudiziaria le cui funzioni sono esercitabili, alle dipendenze e sotto la direzione dell'autorità giudiziaria, all'emergere degli indizi di un fatto penalmente rilevante".

63. Perrone 2022, p. 83.

64. Al paragrafo 5.3.2. della *Guidelines on prohibited artificial intelligence practices* sono indicati, come esempi di sistemi AI che non rientrano nel divieto dell'art. 5 lett. d), le seguenti ipotesi: 1. "Un giudice conduce un'udienza per la custodia cautelare di una persona accusata di un reato grave, per valutare se possano essere applicate misure non detentive. La decisione si basa sulla valutazione di elementi concreti che giustificano la custodia cautelare, come il rischio di reiterazione del reato, fuga o intralcio alle indagini. A supporto, il giudice utilizza uno strumento di valutazione del rischio basato sull'IA, addestrato su dati relativi a precedenti penali in casi simili e su fattori quali età, comportamento sociale, reddito e occupazione"; 2. "Un sistema di IA è utilizzato per supportare la valutazione di un agente nel determinare il rischio che una persona sottoposta a misure alternative violi le condizioni di rilascio o si sottragga alla giustizia, sulla base di comportamenti criminali passati e fatti oggettivi che giustificano il sospetto, come il rispetto delle condizioni di rilascio, esiti di valutazioni psicologiche e raccomandazioni dei servizi sociali. Sulla base di tali informazioni, l'agente decide se mantenere o modificare le condizioni".

65. Venturoli 2022, p. 256.

66. Algieri 2021, p. 730.

aerei siano coinvolti in reati gravi, ai sensi della direttiva (UE) 2016/681, c.d. direttiva PNR. Come messo in luce dalla dottrina, questo divieto rileva quale regola di valutazione della prova che si applica, per ragioni di tutela della libertà individuale e del diritto di difesa, anche alle determinazioni degli organi inquirenti relative ad atti d'indagine per verificare il coinvolgimento criminale[67].

Il richiamo a queste statuizioni della Corte di giustizia, e specificamente alla funzione assegnata alla valutazione umana di strumento di controllo individualizzante ed antidiscriminatorio degli esiti sfavorevoli discendenti dai trattamenti automatizzati[68], conferma come la decisione umana che l'AI predittiva deve supportare debba avere di per sé un'autonoma attendibilità, sulla base di dati oggettivi e verificabili, implicanti una relazione diretta tra il soggetto e il reato.

La predetta verificabilità costituisce, inoltre, requisito che dovrebbe evitare o comunque rendere sindacabili sia fenomeni di *automation bias*, sia quelli di recepimento dell'output per rafforzarne *bias* del giudice, foriere di diseguaglianza[69]. Funzionale a questo duplice ruolo è il diritto, espressamente previsto dall'*AI Act* per le autorità nazionali che devono far rispettare gli obblighi unionali a tutela dei diritti fondamentali, di richiedere in relazione all'uso dei sistemi di AI ad alto rischio dell'allegato III l'accesso a qualsiasi documentazione creata o mantenuta a norma del regolamento[70]. Alla luce di questa disposizione sembra possibile ritenere che l'autorità giurisdizionale, in via di adozione e soprattutto di ricorso del provvedimento supportato dal sistema predittivo, possa accedere ai dati di sviluppo e addestramento per verificare la violazione del diritto alla non discriminazione, autorizzando, a tutela dell'effettività del contraddittorio e dello stesso diritto di difesa, il potenziale reo o soggetto interessato a farlo.

Quanto sopra potrebbe contenere il rischio d'emersione per mezzo dell'AI predittiva di un inaccettabile *Tätertyp*[71], della giustificazione di misure pregiudizievoli nell'azione di contrasto sulla base di pericolosi profili di autori derivanti dalla stigmatizzazione criminale di gruppi o categorie sociali[72], quale versione "intelligente" di un diritto penale del nemico[73].

Queste considerazioni valgono a maggior ragione per i sistemi *pre-crime* e specificamente di *predictive policing*, la cui ammissibilità richiede di distinguere tra quelli che consentono di localizzare le aree di probabile compimento di attività criminali (*hot spots*), a garanzia della tempestività ed efficienza dell'intervento (c.d. *place-based*)[74], e quelli, invece, che identificano coloro che potrebbero commettere reati (c.d. *person-based*)[75].

Per la Corte federale tedesca, chiamata ante *AI Act* a pronunciarsi sul trattamento automatizzato dei dati per finalità di polizia, i *place-based systems* sarebbero ammissibili perché l'interferenza nei diritti fondamentali è lieve, essendo l'analisi o la valutazione dei dati non finalizzata ad approfondimenti personali[76]. In presenza, invece, di questi approfondimenti, la tutela del diritto alla autodeterminazione informativa impone che la base giuridica che ne consente il ricorso fissi pure le condizioni per garantire che l'impatto sui diritti e sulle libertà costituzionali degli individui sia

67. Troisi 2019, p. 178.
68. Espliciti in questi termini i paragrafi 157 e 203 di Corte di giustizia, Grande Sez., 21 giugno 2022, *Ligue des droits humains*, C-817/19.
69. Su questi fenomeni, nonché sulla presenza pure di *bias* strutturali del sistema legale, vedi Ferrara 2025, pp. 144-145.
70. Art. 77, par. 1 dell'*AI Act*.
71. Sull'origine di questo concetto e la sua applicazione nel diritto penale della Germania nazista Bricola 1973, p. 29 ss.
72. Castels Renard 2022, pp. 100-102.
73. Su caratteristiche e contenuti del diritto penale del nemico, dall'elaborazione che si deve Jakobs, e quale paradigma concettuale della politica penale Donini–Papa 2007.
74. Utset 2021, p. 179.
75. Basile 2022, p. 6.
76. *Bundersverfassungsgericht*, I Senato (Presidente Stephan Harbarth),16 febbraio 2023-1BvR 1547/19, 1 BvR 2634/20.

proporzionato al bene giuridico tutelato e al pericolo allo stesso da prevenire[77]. Com'è stato messo in luce con riferimento ad altre pronunce della Corte[78], espressive di analogo orientamento, il predetto diritto all'autodeterminazione informativa "va oltre la tutela della privacy e non si limita ad informazioni sensibili per loro natura" identificandosi con "il potere di determinare, in sé, la divulgazione e l'utilizzo dei [suoi] dati personali, anche se connotati da un contenuto informativo minimo"[79].

A causa dei rischi per diritti anche di questo tipo, è stato sostenuto con riferimento all'*AI Act* che i *person-based systems* siano del tutto vietati[80], mentre quelli *place-based systems* sarebbero ammessi ma laddove "puri", cioè predittivi di un rischio criminale impersonale e fondato su dati spaziali o statistici[81]. Questa tesi appare condivisibile, ancorché forse eccedente rispetto alla portata dell'eccezione prevista dall'art. 5 lett. d), ma non può non essere condivisa per la ragione dirimente che in presenza di sistemi misti non è facile stabilire quale sia stato il fattore determinante (spaziale o personologico) che ha influito sull'output[82].

Nel silenzio della legge n. 132/2025, questione, di contro, che rimane aperta afferisce ancora una volta a quale debba essere l'istituto processuale che dia veste alle risultanze dei sistemi predittivi spaziali ammessi, consentendo di farli transitare nel processo. Prima ancora che per ragioni di garanzia, una critica interazione tra uomo e macchina, imposta dal paradigma *human-centred AI*, impone di concepirli quali prove indiziarie soggette ai requisiti prescritti dall'art. 192 c.p.p.[83]

In generale, come anche recentemente confermato dall'Unesco, "il sistema giudiziario dovrebbe puntare a utilizzare gli strumenti di AI per rafforzare, e non per sostituire, il giudizio umano"[84].

4. *Scraping* e dati biometrici: usi legittimi secondo l'autodeterminazione informativa

Il diritto all'autodeterminazione informativa costituisce il fulcro anche del divieto di cui alla lett. e) dell'art. 5 per i sistemi di AI 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.

Con questo divieto, insieme a quelli di cui alle lett. g) e h), l'*AI Act* copre le tecnologie biometriche applicate alla sicurezza, che sono suddivisibili nelle applicazioni di autenticazione ed in quelle di sorveglianza[85]. Quest'ultime, in particolare, sono state considerate espressione della c.d. *crime society*, di una società che, nell'illusione di controllare la percezione di un rischio reato pervasivo ed onnipresente, ammette strumenti di controllo di massa, che, in realtà, finiscono per alimentare il senso di insicurezza[86].

Con specifico riferimento allo *scraping*, è, soprattutto, evidente la connessione con quel fenomeno che è stato definito di "datificazione" delle nostre esistenze, quale "possibilità di convertire ogni

77. Merler 2023, p. 691.
78. Si tratta delle sentenze del *Bundesverfassungsgericht* del 27 febbraio 2008 sulla c.d. *Online Durchsuchung* e del 2 marzo 2010 sulla *data retention*, con cui sono stati dichiarati incostituzionale rispettivamente il § 5 co. 2, n. 11, della Legge sulla protezione della Costituzione del Nord Reno Westfalia in materia di raccolta e trattamento dei dati degli utenti, e i §§ 113a e 113b del *Telekommunikationsgesetz*, come modificato dalla legge di riforma del settore delle telecomunicazioni e delle altre misure d'indagine sotto copertura. Per un commento ad entrambe le sentenze Flor 2012, p. 7.
79. Flor 2015, p. 235.
80. Barone 2024, p. 1058.
81. Camaldo 2024, p. 244.
82. Per le difficoltà di distinguo per sistemi di questo tipo cfr. il paragrafo 5.3.1. della *Guidelines on prohibited artificial intelligence practices.*
83. Camaldo 2024, p. 245.
84. Unesco, *Guidelines for the use of AI Systems in Courts and Tribunals*, p. 32.
85. Pizzolante 2025, p. 158.
86. Su questa ricostruzione sociologica che si deve a Koops si rinvia, anche per i relativi riferimenti bibliografici, a Galli 2022, p. 121.

aspetto della vita (privata e sociale) in dati digitali da raccogliere e analizzare"[87]. Il diritto all'autodeterminazione informativa protegge questi dati quale propagazione virtuale della nostra personalità, consentendo la tutela anche delle differenti aree informatiche in cui si trovano[88]. Prendendo a prestito le parole d'insigne Maestro "la libertà in rete, tuttavia, non vale solo contro l'invadenza degli Stati, ma si proietta anche verso i nuovi 'signori dell'informazione' che, attraverso le gigantesche raccolte di dati, governano le nostre vite. Di fronte a tutto questo la parola 'privacy' evoca non solo un bisogno d'intimità, ma sintetizza le libertà che ci appartengono nel mondo nuovo dove ormai viviamo"[89].

Con specifico riferimento allo *scraping* non mirato d'immagini facciali, di cui al regolamento in esame, l'inclusione dello spazio aperto d'Internet è espressione di questo retroterra, chiamando in causa, in particolare, la conformità al principio di lealtà del trattamento dati, che è codificato al comma 2 all'art. 8 della Carta europea dei diritti fondamentali[90]. A questo principio sono ispirati gli orientamenti espressi nel caso di *Clearview AI* dal Garante europeo della protezione dei dati e dal nostro Garante privacy. In particolare, quest'ultimo ha sostenuto che la mera accessibilità pubblica delle immagini non è sufficiente a giustificare lo *scraping* in quanto gli interessati non possono ragionevolmente aspettarsi che le proprie immagini vengano utilizzate per finalità di riconoscimento facciale, per cui non hanno manifestato il proprio consenso[91]. Con specifico riferimento al contesto di *law enforcement*, il Garante europeo[92] ha chiarito, inoltre, che se il trattamento iniziale dei dati per finalità private non è conforme al GDPR, le autorità di contrasto non li possono utilizzare in quanto l'obiettivo generale di migliorare l'efficienza nella lotta ai reati gravi non costituisce, di per sé, una giustificazione valida per la raccolta e il trattamento indiscriminato di dati[93].

Il divieto dell'*AI Act* sullo *scraping* non mirato, ponendosi in conformità con questi orientamenti, va concepito alla luce dei principi e criteri del GDPR e della direttiva LED, la quale, peraltro, impone all'art. 10 che il trattamento di dati sensibili operato dalle autorità di contrasto sia informato al criterio della "stretta necessità"[94].

La sensibilità del dato, per i profili anche discriminatori che vi possono essere connessi, è aspetto centrale altresì nel divieto di cui alla lett. g) dell'art. 5, in ordine ai sistemi di categorizzazione biometrica per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; tale divieto non riguarda, però, l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente nell'ambito delle attività di contrasto.

L'*AI Act* definisce i dati biometrici come quelli "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"[95]. Questa nozione si pone ancora una volta in continuità con il GDPR, che vieta l'impiego di questi dati, salvo se, tramite il loro trattamento, con le dovute garanzie, si possa giungere all'identificazione univoca o all'autenticazione di una persona fisica, in presenza del

87. Flor 2012, p. 13.

88. In base al tenore letterale della previsione sono ammissibili trattamenti di dati che avvengano "per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge".

89. Rodotà 2010, p. 342.

90. Belvini 2026, p. 157.

91. Garante Privacy, Ordinanza ingiunzione nei confronti di *Clearview AI* del 10 febbraio 2022, n. 9751362/2022.

92. Garante europeo della protezione dei dati, *Parere sull'uso di Clearview AI da parte di Europol* (Case 2020-0372).

93. In questi termini espliciti le *Guidelines on the use of facial recognition technology in the area of law enforcement*, adottate il 26 aprile 2023 dal Comitato europeo per la protezione dei dati (EDPB).

94. Per l'incompatibilità di questo criterio proprio con forme di *screening* generalizzati via web vedi Belvini 2026, p. 160.

95. Art. 3, n. 34 dell'*AI Act*.

requisito alternativo del consenso esplicito oppure della necessità per ragioni di pubblico interesse[96].

L'area di eccezione ammessa dall'*AI Act* rientra in quest'ultima ipotesi e di conseguenza soggiace agli ulteriori requisiti che sono fissati dal sopracitato art. 10 della direttiva LED[97], operando, ad avviso di chi scrive, a causa della considerazione dei sistemi di etichettatura e filtraggio ammessi come ad alto rischio, come fattore di emersione di ulteriori cautele.

L'autonomia parziale di questa disciplina con riferimento all'area penale comporta, però, anche la permanenza del quadro di pesi e contrappesi che le corti sovranazionali hanno già individuato per la raccolta di dati biometrici da parte delle forze dell'ordine, in conformità ai diritti previsti dagli artt. 7-8 e ai criteri di necessità e proporzionalità dell'art. 52 della Carta europea dei diritti fondamentali, e tenendo in debito conto anche il tipo di tecnologia biometrica utilizzata, nonché la durata della conservazione dei dati biometrici e le categorie di soggetti coinvolti[98].

Sul punto una recente pronuncia della Corte di giustizia ha ribadito come la mera sussistenza di una o più ragioni plausibili di sospetto reato non è sufficiente a giustificare la raccolta di dati biometrici, che non può mai rivestire carattere sistematico[99]. Per la Corte, inoltre, questa raccolta laddove legittimamente operata secondo le disposizioni nazionali, può non essere soggetta ad un periodo massimo di conservazione, purché siano fissati termini periodici per verificare la permanenza della necessità di conservare tali dati[100].

Quanto sopra delinea un quadro frastagliato che forse avrebbe imposto, per le peculiarità dei sistemi di AI in attività di contrasto, l'adozione di previsioni apposite o di specifici meccanismi di raccordo con la disciplina europea sul trattamento dati, come precisata dalla giurisprudenza sovranazionale e dalle Autorità di controllo: l'*over-regulation*, infatti, "è sempre un'arma a doppio taglio, nella misura in cui, se è vero che garantisce l'esistenza di più normative che da fronti diversi proteggono gli stessi diritti, dall'altro, se non ben regolato, rischia di ottenere l'effetto opposto alla finalità iniziale, mettendo a rischio quegli stessi diritti che si prefiggeva di tutelare"[101].

4.1. Il riconoscimento facciale tra impieghi ed eccezioni "proporzionali"

Questa esigenza di equilibri "dinamici" tra sicurezza e diritti fondamentali è rinvenibile anche alla base della disciplina europea sui sistemi d'identificazione biometrica. Per comprendere a pieno le differenze di regolamentazione adottate, bisogna partire dalla distinzione tra sistemi di riconoscimento facciale in tempo reale e quelli da remoto (*enterprise*). Nel primo caso la comparazione con i contenuti di una banca dati predefinita avviene contestualmente alla cattura delle immagini, mentre nella seconda versione è svolta a posteriori.

Pur non generando forme di sorveglianza di massa, i sistemi di riconoscimento facciale *enterprise* non sono indenni da rischi o da margini di errore; per questo, in base al combinato disposto degli artt. 5, lett. h), e 26 del regolamento europeo[102], sono consentiti, ma nel rispetto di precise condizioni.

In particolare, previa autorizzazione dell'autorità competente, risultano, oltre che soggetti ai requisiti generali previsti per tutti i sistemi ad

96. Mollo 2024, p. 108, che precisa che l'*AI Act* non può costituire in ogni caso il fondamento giuridico per il trattamento dei dati personali.

97. Per il considerando 94 dell'*AI Act* l'uso in attività di contrasto soggiace a tutti i principi di cui all'articolo 4, paragrafo 1, della Direttiva (UE) 2016/680, tra cui liceità, correttezza e trasparenza, determinazione delle finalità, esattezza e limitazione della conservazione.

98. Sugli orientamenti adottati sul punto dalla Corte EDU vedi Pizzolante 2025, p. 182.

99. Corte di giustizia, 19 marzo 2026, C-371/24.

100. Corte di giustizia, 20 novembre 2025, C57/23.

101. Falletta–Marsano 2024, p. 11.

102. L'art. 26 dell'*AI Act* precisa che "in nessun caso tale sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori è utilizzato a fini di contrasto in modo non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa".

alto rischio, impiegabili solo nell'ambito d'indagini su uno specifico reato per la ricerca mirata di una persona che sia stata per questo condannata o sia sospettata di averlo commesso[103]. Alla luce del considerando 95 il carattere mirato comporta, inoltre, limiti sia sul luogo e sull'ambito temporale di utilizzo sia sugli input che possono alimentare il sistema, da individuare in un set di dati chiuso di filmati acquisiti legalmente. Aspetto ulteriormente interessante è quello relativo alla fissazione da parte del regolamento di quella che è stata definita "una regola di utilizzabilità degli output di questi sistemi di identificazione biometrica"[104], in forza della quale nessuna decisione che produce effetti giuridici negativi in capo a una persona può fondarsi esclusivamente su di essi.

Ne fuoriesce così un modello *rights driven*[105] particolarmente stringente e munito di un livello di specificità tale da impattare direttamente sul piano nazionale. Invero, in questa prospettiva, questione che andrebbe preliminarmente chiarita è se, salva l'ipotesi d'identificazione iniziale di un sospettato che tale sia in base a previi fattori oggettivi, negli altri casi l'assenza di autorizzazione si traduca sempre nel divieto di utilizzabilità[106]. La risposta positiva a questo quesito travolgerebbe anche impieghi del nostro sistema SARI *enterprise* ammessi dal nostro Garante privacy sul presupposto che questo strumento coadiuva e non sostituisce l'attività dell'operatore di polizia in processi d'identificazione, come quelli ai sensi dell'art. 349 c.p.p.[107] Un tale esito può sembrare eccessivo, a maggior ragione se pensiamo che il regolamento funge da "statuto minimo", che sarebbe derogabile a livello nazionale solo con disposizioni più restrittive[108].

Questo aspetto va a maggior ragione tenuto presente con riguardo alla disciplina europea sui sistemi di identificazione biometrica in tempo reale in spazi accessibili al pubblico: ferma l'immediata operatività del divieto in sé, per le ipotesi d'impiego eccezionalmente ammesse la disciplina sovranazionale non è immediatamente applicabile, ma fissa degli standard che per la valenza garantistica assiologica sono già vincolanti.

La delega al legislatore dello Stato membro per l'adozione della relativa disciplina nazionale conforme a questi standard, è, infatti, una delega "limitata", che può operare nel *range* dei requisiti abilitativi sovranazionali fissati dall'art. 5 dell'*AI Act*[109]. Questi requisiti, peraltro, ancorando il principio di proporzionalità ad un fondamento legale, migliorano, in forza della predetta formalizzazione, la capacità di resistenza dei diritti contro

103. Questa norma prevede, peraltro, a favore di una parziale *disclosure*, che ciascun uso di tali sistemi di IA ad alto rischio è documentato nel relativo fascicolo di polizia e messo a disposizione della pertinente autorità di vigilanza del mercato e dell'autorità nazionale per la protezione dei dati, su richiesta, escludendo la divulgazione di dati operativi sensibili relativi alle attività di contrasto.

104. Vasta 2024, p. 284.

105. Per la differenza con il modello cinese *state driven* e con quello americano *market driven* vedi Bottari–Currao 2026, p. 4 ss.

106. Cesari 2026, p. 185.

107. Vele 2026, p. 30.

108. De Martis 2025, p. 183.

109. Esplicito in questo senso è il paragrafo 5 dell'art. 5 dell'*AI Act*, che stabilisce quanto segue: "Uno Stato membro può decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota 'in tempo reale' in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni di cui al paragrafo 1, primo comma, lettera h), e ai paragrafi 2 e 3. Gli Stati membri interessati stabiliscono nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo e comunicazione ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati al paragrafo 1, primo comma, lettera h), compresi i reati di cui alla lettera h), punto iii), le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto. Gli Stati membri notificano tali regole alla Commissione al più tardi 30 giorni dopo la loro adozione. Gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota".

derive securitarie rispetto alle quali l'AI potrebbe segnare un punto di non ritorno.

Nello specifico, l'articolato impianto normativo in questo modo non intende solo evitare la compromissione dei già richiamati diritti alla privacy e alla non discriminazione, ma anche di quelle libertà universalmente riconosciute – da quella di movimento a quella manifestazione[110] – che sono funzionali a preservare la dignità umana nel contesto di una società democratica[111].

Ciò comporta a livello nazionale che, nonostante la proroga fino al 31 dicembre 2027 del divieto di questi sistemi di riconoscimento *real time* con moratoria per quelli effettuati a certe condizioni dall'autorità giudiziaria[112], nel silenzio della legge n. 132/2025 questa moratoria sia travolta dal divieto sovranazionale fino all'emanazione di un'apposita disciplina che regolamenti gli usi eccezionali nel rispetto dei criteri fissati dal legislatore europeo.

Venendo ai contenuti di questi criteri, salvo situazioni di urgenza debitamente giustificate[113], pre-condizione europea necessaria per gli impieghi ammessi dei sistemi di riconoscimento facciale *real time* in luoghi aperti al pubblico è che essi siano autorizzati, previa registrazione nella relativa banca dati e completamento della valutazione d'impatto sui diritti fondamentali[114], da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro sulla base di prove oggettive o indicazioni chiare. Su scia della giurisprudenza sovranazionale adottata per altri sistemi d'indagine tecnologica, è possibile ritenere che la legge nazionale, che dovrà prevedere nel dettaglio l'iter di autorizzazione, richieda il vaglio preventivo del giudice su richiesta del pm[115].

In ogni caso, questo vaglio deve avvenire, sulla base del testo sovranazionale, nel rispetto delle regole degli Stati membri che fissano limitazioni temporali, geografiche e personali e deve avere ad oggetto la necessità e la proporzionalità della misura rispetto ad almeno una delle seguenti finalità: (a) la ricerca mirata di persone scomparse e di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale; (b) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; (c) la localizzazione o identificazione di una persona sospettata, indagata o ricercata per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

Queste tre ipotesi costituiscono delle ragioni giustificative eccessivamente ampie, richiamano

110. In relazione a questa libertà Borgia 2021, p. 15, mette in luce il c.d. *chilling-effect* che può essere generato da questi sistemi di AI, quale effetto inibitore alla partecipazione a manifestazioni pubbliche per il timore di essere identificati.

111. Cavaliere 2020, p. 8.

112. Proroga prevista dall'art. 2, comma 6-*quater*, del d.l. n. 200/2025, c.d. "Decreto Milleproroghe 2026", convertito nella legge n. 26/2026 del 27 febbraio 2026.

113. Il paragrafo 3, ultima parte, dell'art. 5 dell'*AI Act*, stabilisce, in presenza di situazioni di questo tipo, che è possibile iniziare ad usare il sistema senza autorizzazione, a condizione, però, che sia richiesta entro 24 ore. Se tale autorizzazione è respinta, l'uso deve essere interrotto con effetto immediato e cancellazione dei relativi dati.

114. Questa valutazione è prevista dall'art. 27 dell'*AI Act*, il quale indica tra gli elementi che devono essere considerati: "c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13; e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; f) le misure da adottare qualora tali rischi si concretizzino".

115. Borgia 2021, p. 22. In questa prospettiva anche il paragrafo 10.2.2.2. delle *Guidelines*, per cui "l'indipendenza richiesta dall'articolo 5, paragrafo 3, dell'AI Act (…) implica che l'autorità che autorizza debba essere indipendente dall'autorità che utilizza il sistema RBI. Ciò si applicherebbe non solo alla polizia, ma anche ai casi di giudici istruttori o pubblici ministeri che supervisionano il lavoro della polizia e l'uso di sistemi RBI per i quali è richiesta un'autorizzazione".

"scenari emergenziali" che possono consentire praticamente sempre il ricorso "anche ai mezzi più controversi per conseguire lo scopo prefissato"[116]. In questo senso particolarmente rilevante è la condizione di cui alla lett. (b): i requisiti di attualità e realtà, previsti per la minaccia o l'attacco terroristico, ne impongono una considerazione *case by case*, alla luce delle specificità della situazione concreta, con possibilità, già ammessa per altri strumenti investigativi invasivi, di poterli ritenere sussistenti anche quando non si possa stabilire con sufficiente probabilità che la minaccia o l'attacco si concretizzeranno in futuro[117].

Alla luce, poi del considerando 33 dell'*AI Act* il concetto di minaccia imminente alla vita o all'incolumità fisica delle persone è declinabile in modo da includere anche quella alle infrastrutture critiche, da cui possa discendere un grave danno alla popolazione o all'esercizio delle funzioni fondamentali dello Stato. Questa estensione appare ragionevole in considerazione di quelli che oggi costituiscono modalità frequenti, anche in forma, peraltro, *cyber*[118] degli attacchi – di matrice terroristica o addirittura di *ius ad bellum*[119] – rivolti alle infrastrutture di settori come sanità ed energia. Sembra rispondere alla medesima logica spiccatamente preventiva-securitaria l'elencazione dei reati di cui all'allegato II[120] del regolamento, per cui è ammesso ai sensi della lett. (c) la localizzazione o identificazione di condannato-sospettato mediante riconoscimento biometrico *real time*.

Come chiarito dalla Commissione si tratta o di "reati europei", rientranti nelle ipotesi di cui all'articolo 83 TFUE, che legittimano una competenza penale europea concorrente[121], o di quelli per cui può essere emesso un mandato d'arresto europeo[122]. La possibile, ulteriore considerazione di questi reati come gravi ai sensi anche della giurisprudenza sovranazionale[123] potrebbe non escludere censure, che, ad avviso di chi scrive, non afferiscono alla riconoscibile lesività degli stessi in astratto, quanto più che altro al rischio di (dis) armonizzazione applicative tra gli Stati. Nello specifico, l'indicazione nominale è operata mediante macro-categorie che si prestano più ad indicare forme di criminalità che reati, al fine di abbracciare la complessa "fenomenologia concreta dei comportamenti 'criminologicamente rilevanti'"[124]. Non sembra essere dirimente rispetto a ciò l'indicazione della soglia di pena di almeno quattro anni, nonostante si tratti di un parametro generalmente impiegato e certamente conforme al principio proporzionalità. Il riferimento alla pena ha, infatti, una valenza in termini, in particolare, di congruità che dovrebbe sussistere tra la sua entità e la gravità che si attribuisce alla sfera di lesività

116. Colacurci 2022, p. 21.

117. Flor 2015, p. 236.

118. Per un'analisi statica su attacchi di questo tipo nel corso del 2025 si rinvia al Rapporto Clusit 2026.

119. Gabrielli 2025, p. 80 ss.

120. Questi reati sono: terrorismo, 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.

121. Questa competenza è anche definita indiretta, in quanto è devoluto al legislatore europeo un giudizio di meritevolezza di pena senza diretta potestà punitiva, dovendo le "norme minime" relative alla definizione dei reati e delle sanzioni passare attraverso il contributo di recepimento del singolo Stato membro. Senza alcuna pretesa di esaustività, in proposito, vedi Picotti 2011, p. 207 ss.; Grasso 2011, p. 2324 ss.; Paonessa 2009, p. 237 ss.

122. In proposito il paragrafo 9.3.4. delle *Guidelines*.

123. Sulle pronunce della Corte di giustizia, che – con specifico riferimento alla *data retention* – hanno esemplificato le fattispecie rientranti nella nozione di criminalità grave, riferendosi alla criminalità organizzata e al terrorismo, vedi Luberto 2025, p. 74.

124. Così, con riguardo all'allora normazione comunitaria di diritto penale dell'economia, Paliero 2000, p. 489.

selezionata[125], quale manifestazione della ragionevolezza intrinseca della fattispecie. Da quanto sopra, consegue, pertanto, che se è corretto il riferimento al limite massimo, perché espressione del disvalore del tipo di reato, non è condivisibile il *quantum* di questo limite (quattro anni), che appare eccessivamente basso; confrontato con il nostro ordinamento, potrebbe consentire di ritenere operante l'eccezione in esame per reati, per cui non sarebbe ammissibile procedere nemmeno alle intercettazioni.

Di tutt'altra valenza è la funzione garantistica attribuibile, invece, all'ulteriore condizione di una prognosi *ex ante* che l'autorità è chiamata a svolgere in ordine sia ai danni che deriverebbero dall'omesso impiego di questi sistemi di *AI real time*, sia alle conseguenze discendenti, di contro, dal suo utilizzo per i diritti e le libertà di tutte le persone interessate. In entrambi i casi questi effetti vanno valutati in termini di gravità, probabilità ed entità.

La prima parte di questo duplice giudizio controfattuale è, soprattutto, valorizzabile per far emergere quella dimensione di lesività effettiva, che rischia di essere dispersa dalla elencazione dei sopra definiti macro-reati rispetto ai quali può operare la finalità di cui alla lett. (c).

Si evidenzia che questi reati sono, peraltro, connotati da un marcata anticipazione dell'intervento penale[126], con la conseguenza che la verifica in esame potrebbe fungere da utile argine operativo.

In questa direzione si segnala, inoltre, che il richiamo all'offensività in concreto, operando qui come fattore di ammissione o esclusione del sistema intelligente di sorveglianza, non si espone a quelle censure che gli sono riferite quando funge, invece, da criterio di riduzione del "penale", consentendo al giudice di escludere dalla sfera d'azione della fattispecie le condotte inoffensive che vi rientrerebbero[127]. Quest'ultimo uso entra in tensione con la formalità della legalità penale, nella sua funzione di presidio anche sostanziale, che opera sia a "limitazione dell'attività valutativa del giudice nell'identificazione dei fatti rilevanti", sia ad "orientamento del comportamento del cittadino"[128].

Questa tensione non si registra, invece, per la offensività qui in esame: laddove ricorra la condizione cui alla lett. (c) la valutazione di dannosità sociale va riferita, infatti, ad una cornice d'interessi o beni che, anche se con i limiti segnalati, è stata delineata dal legislatore europeo, con la selezione dei reati di cui all'allegato II.

In realtà, anche in ordine alle altre finalità che consentono il ricorso al riconoscimento facciale *real time* (ricerca vittime-minaccia, attacco terroristico), il duplice giudizio controfattuale funge, comunque, da criterio esegetico applicativo, che non è estraneo al substrato di fondo che anima il principio di offensività[129].

La verifica imposta, pur non essendo riferibile alla prospettiva tradizionale del bene giuridico, meno in linea con l'*acquis* comunitario[130], sposta, di fatto, l'attenzione sul sacrificio dei diritti e delle libertà di tutte i soggetti coinvolti, compresi i terzi estranei, anche se in termini probabilistici-potenziali.

La considerazione di questo sacrificio non è avulsa dell'art. 52 della Carta europea dei diritti fondamentali. Stando alla formulazione testuale di questa previsione, la valutazione di necessità e idoneità della misura limitativa va infatti, condotta, secondo il criterio alternativo delle "finalità di interesse generale riconosciute dall'Unione" e della "esigenza di proteggere i diritti e le libertà altrui". Rispetto ad entrambi i criteri, il giudizio controfattuale qualitativo-quantitativo previsto dal regolamento consente il ricorso al mezzo investigativo intelligente in condizioni oggettive che devono essere particolarmente pregnanti.

In senso critico si potrebbe obiettare sul punto che, in realtà, con questo duplice accertamento

125. Bricola 1965, p. 311.

126. Sull'anticipazione dell'intervento penale con riguardo ai reati di terrorismo si rinvia a Risicato 2019, p. 50 ss.

127. Cadoppi 2022, p. 258.

128. Paonessa 2017, p. 308.

129. A favore di questa omogeneità di fondo tra l'offensività e i parametri di proporzionalità e ragionevolezza Fornasari 2018, p. 1529.

130. Diffusamente su questi aspetti De Lia 2019, p. 34.

controfattuale (danno da non impiego – compromissione dei diritti e le libertà di tutte le persone interessate dall'impiego) vengano semplicemente esplicitati i fattori di quello che rimane, comunque, un giudizio discrezionale di bilanciamento tra valori, tradizionalmente riferibile al principio di proporzionalità.

È vero che l'*AI Act* non muta la valenza sostanziale di questo principio, ma nel chiamarlo in causa nel suo ruolo di "conciliatore" tra "i due grandi criteri dell'ordine sociale: la libertà individuale e la sicurezza sociale, l'individuo e lo Stato"[131], gli conferisce, però, una consistenza propriamente fattuale.

Questa consistenza opera a favore di tutti i soggetti interessati, dal potenziale reo alle vittime, perché con riferimento agli "occulti" ed "imprevedibili" sistemi intelligenti comporta una maggiore ponderazione della decisione umana, con ricadute in termini di trasparenza e controllabilità della stessa e a favore di un diritto penale umano e contenibile.

Riferimenti bibliografici

L. Algieri (2021), *Intelligenza artificiale e polizia predittiva*, in "Diritto penale e processo", 2021, n. 6

A.C. Amato Mangiameli (2023), *Tecno-diritto/regolazione*, in A.C. Amato Mangiameli, G. Saraceni (a cura di), "Cento e una voce di informatica giuridica", Giappichelli, 2023

G.M. Baccari, C. Conti (2021), *La corsa tecnologica tra Costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in "Diritto penale e processo", 2021, n. 6

S. Barona Vilar (2019), *Justicia penal desde la globalizaciòn y la postmodernidad hasta la neomodernidad*, in "Revista Boliviana de Derecho", 2019, n. 27

G. Barone (2024), *Artificial Intelligence Act: un primo sguardo al regolamento che verrà*, in "Cassazione penale", 2024, n. 3

F. Basile (2022), *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in G. Balbi, F. De Simone, A. Esposito, S. Manacorda (a cura di), "Diritto penale e intelligenza artificiale. Nuovi scenari", Giappichelli, 2022

L. Belvini (2026), *La disciplina dei software di riconoscimento facciale: rischi e prospettive*, in "Processo penale e giustizia", 2026, n. 1

C. Bernasconi (2022), *Dalla vittimologia al vittimocentrismo: cosa resta della tradizione reocentrica?*, in "discrimen.it", 15 marzo 2022

C. Bernasconi (2019), *A proposito di Caino*, in "discrimen.it", 25 settembre 2019

K. Blount (2021), *Applying the presumption of innocence to policing with AI*, in G. Vermeulen, N. Peršak, N. Recchia (Eds.), "Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice", Maklu Publishers, 2021

R. Borges Blàzquez (2021), *Inteligencia artifical y proceso penal*, Cizur Menor, 2021

G. Borgia (2021), *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in "legislazionepenale.it", 11 dicembre 2021

M. Bottari, E. Currao (2026), *Riconoscimento facciale: tecnologie che corrono, diritti che frenano. Il caso italiano del Faceboarding*, in "federalismi.it", 25 marzo 2026

F. Bricola (1973), *Teoria generale del reato*, in "Novissimo Digesto italiano", XIX, 1973

F. Bricola (1965), *La discrezionalità nel diritto penale*, Giuffrè, 1965

131. Falato 2018, p. 27.

A. Cadoppi (2022), *Il "reato penale". Teorie e strategie di riduzione della criminalizzazione*, Edizioni Scientifiche Italiane, 2022

Camaldo (2024), *Intelligenza Artificiale e investigazione penale predittiva*, in "Rivista Italiana di Diritto e Procedura Penale", 2024, n. 1

A. Camon (2025), *Intelligenza artificiale, indagini preliminari e diritti di libertà*, in "Cassazione penale", 2025, n. 10

M.C. Canato (2024), *Verso il superamento del "legal rick" europeo: Intelligenza artificiale e approccio proporzionale al rischio*, in "legislazionepenale.it", 31 luglio 2024

O. Caramaschi (2025), *Il costituzionalismo al cospetto dell'intelligenza artificiale: nuove sfide, quali soluzioni?*, in "Rivista italiana di informatica e diritto", 2025, n. 1

C. Castels Renard (2022), *Human Rights and Algorithmic Impact Assessment for Predictive Policing*, in H.W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (Eds.), "Constitutional Challenges in the Algorithmic society", Cambridge University Press, 2022

S. Cavaliere (2020), *Il concetto di dignità umana nel diritto internazionale ed europeo: una breve nota ricostruttiva*, in "Euro-Balkan Law and Economics Review", 2020, n. 2

C. Cesari (2026), *Nuove tecnologie, dati biometrici e procedimento penale*, Cedam, 2026

A. Chelo (2025), *Tutela della libertà morale nella formazione della prova penale*, Cedam, 2025

C.M. Christensen, M.E. Raynor, R. McDonald (2015), *What Is Disruptive Innovation? Twenty years after the introduction of the theory, we revisit what it does – and doesn't – explain*, in "Harvard Business Review", 2015, n. 12

M. Colacurci (2022), *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in "sistemapenale.it", 12 settembre 2022

L.M. Colone, M. Esposito, L. Meglio, G. Pagnanelli (2023), *Reati "spia" di femminicidio e pratiche locali di contrasto alla violenza di genere*, in "Sicurezza e scienze sociali", 2023, n. 3

F. Consulich (2024), *Il diritto penale al tempo dell'intelligenza artificiale. Prospettive punitive nazionali dopo l'AI ACT*, in "dirittodidifesa.eu", 17 dicembre 2024

A. De Lia (2019), *"Ossi di seppia"? Appunti sul principio di offensività*, in "Archivio penale", 2019, n. 2

F. De Martis (2025), *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, Cedam, 2025

P. Di Nicola Travaglini (2025), *Il femminicidio esiste ed è un delitto di potere*, in "Sistema penale", 2025, n. 3

M. Donini, M. Papa (2007), *Diritto penale del nemico*, Giuffrè, 2007

F. Falato (2018), *La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale*, in "Archivio penale", 2018, n.1

P. Falletta, A. Marsano (2024), *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in "Rivista italiana di informatica e diritto", 2024, n. 1

A. Ferrara (2025), *The error in predictive justice systems. Challenges for justice, freedom, and human-centrism under EU law*, in "Freedom, Security & Justice: European Legal Studies", 2025, n. 2

R. Flor (2022), *Data retention, accertamento e repressione dei reati e tutela dei diritti fondamentali dell'individuo: fiat iustitia ruat cealum*, in R. Flor, S. Marcolini (a cura di), "Dalla data retention alle indagini ad alto contenuto tecnologico", Giappichelli, 2022

R. Flor (2015), *Dalla 'Data retention' al diritto all'oblio. dalle paure orwelliane alla recente giurisprudenza della corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive 'de jure*

condendo'?, in G. Resta, V. Zeno-Zencovich, "Il diritto all'oblio su Internet dopo la sentenza Google Spain", Roma TrE-Press, 2015

R. Flor (2012), *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi' diritti fondamentali nell'era di Internet*, in "Diritto penale contemporaneo", 20 settembre 2012

G. Fornasari (2018), *Offensività e post modernità: un binomio inconciliabile?*, in "Rivista Italiana di Diritto e Procedura Penale", 2018, n. 3

G. Gabrielli (2025), *La governance internazionale della cybersicurezza: cyber attacchi contro infrastrutture critiche nella prospettiva dello jus ad bellum*, in R. Brighi, G. Adinolfi (a cura di), "Governare la sicurezza degli (eco)sistemi cyberfisici. Regolamentazione, diritti e politiche", Giappichelli, 2025

B. Galgani (2019), *Giudizio penale, habeas data e garanzie fondamentali*, in "Archivio penale", 2019, n. 1

F. Galli (2022), *Law enforcement and Data driven Predictions at National and EU Level*, in H.W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (Eds.), "Costitutional Challenges in the Algorithmic society", Cambridge University Press, 2022

A. Giraldi (2020), *Intelligenza artificiale e predictive policing nella rinnovata fase d'indagine*, in A. Massaro (a cura di), "Intelligenza artificiale e giustizia penale", 2020

G. Grasso (2011), *Il Trattato di Lisbona e le nuove competenze penali dell'Unione europe*a, in "Studi in onore di Mario Romano", Iovene, 2011

S. Hassan, P. De Filippi (2017), *The Expansion of Algorithmic Governance: From Code is Law to Law is Code*, in "Field Actions Science Reports", Special Issue, 2017, n. 17

F. Lazzeri (2025), *In G.U. la L. 2 dicembre 2025, n. 181 (c.d. Legge sul femminicidio): una panoramica dei profili penalistici sostanziali e processuali*, in "sistemapenale.it", 3 dicembre 2025

L. Lessing (2000), *Code is law. On liberty in cyberspace*, in "Harvard magazine", 2000

M. Luberto (2025), *La riforma della data retention a fini di contrasto della criminalità Tra evoluzione tecnologica e garanzia dei diritti*, in "i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale", 2025, n. 2

L. Luparia, G. Fiorelli (2022), *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in "Diritto penale contemporaneo", 2022, n. 2

L. Macrì (2025), *I primi passi dell'Italia verso l'impiego dell'IA nel processo penale e il calcolo del rischio di recidiva*, in "Giurisprudenza Penale", 2025, n. 2

P. Maggio (2017), *Giustizia penale e tratta di esseri umani: i risvolti processuali della "vulnerabilità"*, in "Rivista di medicina legale", 2017, n. 2

V. Manes (2020), *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in "discrimen.it", 15 maggio 2020

F. Mantovani (1992), *Principi Fondamentali del Diritto Penale della Libertà*, in "Derecho Penal y Criminologia", 1992, n. 14

A. Massaro (2025), *Riflessioni sul disegno di legge in materia di femminicidio*, in "sistemapenale.it", 25 giugno 2025

E. Mensa, D. Colla, M. Dalmasso, M. Giustini, C. Mamo, A. Pitidis, D.P. Radicioni (2020), *Violence detection explanation via semantic roles embeddings*, in "BMC Medical Informatics and Decision Making", 2020, n. 1

M. Merler (2023), *La corte costituzionale tedesca si pronuncia sul trattamento automatizzato dei dati in contesti di polizia*, in "Giornale di diritto amministrativo", 2023, n. 5

F. Mollo (2024), *Il trattamento dei dati biometrici nell'IA Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale*, in "federalismi.it", 28 novembre 2024

D. Morondo Taramundi (2025), *Prevenzione versus predizione del rischio: l'uso del programma semi-automatizzato di decisione VioGén in Spagna*, in "Diritto & Questioni pubbliche", 2025, n. XXV

D. Negri (2016), *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in "Archivio penale", 2016, n. 2

W. Nocerino (2020), *Le nuove tecniche di investigazione proattiva e le ricadute processuali – prima parte*, in "Studium iuris", 2020, n. 7-8

C. Paliero (2000), *La fabbrica del Golem. Progettualità e metodologia per la «Parte Generale» di un Codice Penale dell'Unione Europea*, in "Rivista Italiana di Diritto e Procedura Penale", 2000

A.U. Palma (2020), *Le "prove di verità" e la libertà morale del dichiarante*, in "Archivio penale", 2020, n. 1

C. Paonessa (2017), *Parola e Linguaggio nel diritto penale: la garanzia della forma oltre il formalismo*, in "Studi Senesi", vol. CXXIX, 2017

C. Paonessa (2009), *Gli obblighi di tutela penale. La discrezionalità legislativa nella cornice dei vincoli costituzionali e comunitari*, Edizioni ETS, 2009

L. Parodi (2025), *La "gravità dell'ingerenza" nel prisma della proporzionalità: nuovi equilibri in tema di data retention*, in "sistemapenale.it", 7 marzo 2025

G. Pavan (2013), *Tutela penale della vittima nel diritto penale*, in "Digesto delle discipline penalistiche", agg. VII, Utet Giuridica, 2013

C. Pecorella (2025), *Perché può essere utile una fattispecie di femminicidio*, in "sistemapenale.it", 2 giugno 2025

D. Perrone (2022), *La prognosi postuma tra distorsioni cognitive e software predittivi. Limiti e possibilità del ricorso alla "giustizia digitale integrata" in sede di accertamento della colpa*, Giappichelli, 2022

L. Picotti (2011), *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, in G. Grasso, L. Picotti, R. Sicurella (a cura di), "L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona", Giuffrè, 2011

E. Pietrocarlo (2023), *Predictive policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali*, in "sistemapenale.it", 28 settembre 2023

G. Pizzolante (2025), *Il quadro giuridico europeo sulla sorveglianza biometrica*, in "Rivista di diritti comparati", 2025, n. 3

L. Pulito (2025), *Algoritmi predittivi e valutazione della pericolosità sociale: livelli di rischio alla luce dell'AI Act e prospettive interne di impiego*, in "Archivio penale", 2025, n. 3

L. Pulito (2024), *Il contributo dell'intelligenza artificiale simbiotica nella protezione delle vittime vulnerabili e nel contrasto della violenza di genere*, in "BioLaw Journal", 2024, n. 1

S. Quattrocolo (2025), *Intelligenza artificiale e processo penale: le novità dell'AI Act*, in "Diritto di difesa", 16 gennaio 2025

L. Risicato (2019), *Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?*, Giappichelli, 2019

S. Rodotà (2010), *Una Costituzione per Internet?*, in "Politica del diritto", 2010, n. 3

G. Ruggiero (2023), *I principi del diritto penale: controlimiti nel tempo del "disagio della democrazia"*, in "Rivista Italiana di Diritto e Procedura Penale", 2023, n. 4

F. Sgubbi (2019), *Diritto penale totale. Punire senza legge, senza verità, senza colpa. Venti tesi*, Il Mulino, 2019

S. Signorato (2016), *Tipologie e caratteristiche delle cyber investigations in un mondo globalizzato*, in "Diritto penale contemporaneo", 2016, n. 3

P. Sorbello (2019), *Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto*, in "Diritto penale contemporaneo", 2019, n. 2

I. Speziale (2025), *Le linee guida della Commissione europea in materia di pratiche di intelligenza artificiale vietate*, in "Contratto e impresa", 2025, n. 2

M. Torre (2019), *Indagini informatiche e principio di proporzionalità*, in "Processo penale e giustizia", 2019, n. 6

P. Troisi (2019), *Passenger Name Records, privacy e accertamento penale*, in "Processo penale e giustizia", 2019, n. 1

M.A. Utset (2021), *Predictive policing and criminal law*, Taylor e Francis ebook, 2021

V. Vasta (2024), *Diritto dell'Unione Europea e Intelligenza Artificiale. Riflessi sul procedimento penale*, in "Rivista Italiana di Diritto e Procedura Penale", 2024, n. 1

M. Venturoli (2022), *Le misure sospensivo-probatorie nella fase esecutiva della pena tra criticità e prospettive di riforma*, in "Rivista Italiana di Diritto e Procedura Penale" 2022, n. 1

M. Venturoli (2021), *La "centralizzazione" della vittima nel sistema penale contemporaneo tra impulsi sovranazionali e spinte populistiche*, in "Archivio penale", 2021, n. 1

M. Venturoli (2017), *Vittima. Profili di diritto penale*, in Treccani–Diritto on line, 2017

A. Vele (2026), *Identificazione, intelligenza artificiale e riconoscimento facciale ai sensi dell'art. 349 c.p.p.*, in "Archivio penale", 2026, n. 1

F. Viganò (2023), *Diritto penale e diritti della persona*, in "sistemapenale.it", 13 marzo 2023

A. Ziroldi (2019), *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in "questionegiustizia.it", 18 ottobre 2019