



# Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

---

REVISTA TRIMESTRAL DE DERECHO PENAL  
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

4/2025

## EDITOR-IN-CHIEF

Gian Luigi Gatta

## EDITORIAL BOARD

*Italy:* Mitja Gialuz, Antonio Gullo, Guglielmo Leo, Luca Luparia, Francesco Mucciarelli, Francesco Viganò

*Spain:* Jaume Alonso-Cuevillas, Sergi Cardenal Montraveta, David Carpio Briz, Joan Queralt Jiménez

*Chile:* Jaime Couso Salas, Mauricio Duce Julio, Héctor Hernández Basualto, Fernando Londoño Martínez

## MANAGING EDITORS

Silvia Bernardi, Beatrice Fragasso

## EDITORIAL STAFF

Enrico Andolfatto, Enrico Basile, Emanuele Birritteri, Carlo Bray, Jorge Hernan Fernandez Mejias, Elisabetta Pietrocarlo, Rossella Sabia, Tommaso Trinchera

## EDITORIAL ADVISORY BOARD

María Acale Sánchez, Rafael Alcacer Guirao, Alberto Alessandri, Silvia Allegrezza, Chiara Amalfitano, Giuseppe Amarelli, Coral Arangüena Fanego, Lorena Bachmaier Winter, Roberto Bartoli, Fabio Basile, Hervé Belluta, Teresa Bene, Alessandro Bernardi, Carolina Bolea Bardon, Manfredi Bontempelli, Nuno Brandão, David Brunelli, Silvia Buzzelli, Alberto Cadoppi, Pedro Caeiro, Michele Caianiello, Lucio Camaldo, Stefano Canestrari, Francesco Caprioli, Claudia Marcela Cárdenas Aravena, Raúl Carnevali, Marta Cartabia, Fabio Cassibba, Donato Castronuovo, Elena Maria Catalano, Mauro Catenacci, Antonio Cavaliere, Massimo Ceresa Gastaldo, Mario Chiavario, Federico Consulich, Mirentxu Corcoy Bidasolo, Roberto Cornelli, Cristiano Cupelli, Norberto Javier De La Mata Barranco, Angela Della Bella, Jacopo Della Torre, Cristina de Maglie, Gian Paolo Demuro, Miguel Díaz y García Conlledo, Francesco D'Alessandro, Marcello Daniele, Ombretta Di Giovine, Emilio Dolcini, Jacobo Dopico Gomez Áller, Patricia Faraldo Cabana, Silvia Fernández Bautista, Javier Gustavo Fernández Terruelo, Marcelo Ferrante, Giovanni Fiandaca, Gabriele Fornasari, Novella Galantini, Benedetta Galgani, Alessandra Galluccio, Percy García Caverro, Loredana Garlati, Glauco Giostra, Víctor Gómez Martín, José Luis Guzmán Dalbora, Ciro Grandi, Giovanni Grasso, Giulio Illuminati, Roberto E. Kostoris, Máximo Langer, Juan Antonio Lascuraín Sánchez, Maria Carmen López Peregrín, Sergio Lorusso, Paola Maggio, Vincenzo Maiello, Ezequiel Malarino, Francisco Maldonado Fuentes, Stefano Manacorda, Juan Pablo Mañalich Raffo, Enrico Maria Mancuso, Vittorio Manes, Grazia Mannozi, Teresa Manso Porto, Luca Marafioti, Joseph Margulies, Enrico Marzaduri, Luca Masera, Jean Pierre Matus Acuña, Anna Maria Maugeri, Oliviero Mazza, Iván Meini, Alessandro Melchionda, Chantal Meloni, Melissa Miedico, Vincenzo Militello, Fernando Miró Linares, Vincenzo Mongillo, Adán Nieto Martín, Renzo Orlandi, Magdalena Ossandón W., Francesco Palazzo, Carlenrico Paliero, Michele Papa, Raphaële Parizot, Claudia Pecorella, Marco Pelissero, Lorenzo Picotti, Carlo Piergallini, Oreste Pollicino, Domenico Pulitanò, Serena Quattrocchio, Tommaso Rafaraci, Paolo Renon, Lucia Risicato, Mario Romano, María Ángeles Rueda Martín, Carlo Ruga Riva, Stefano Ruggeri, Francesca Ruggieri, Dulce Maria Santana Vega, Marco Scoletta, Sergio Seminara, Paola Severino, Nicola Selvaggi, Rosaria Sicurella, Jesús Maria Silva Sánchez, Carlo Sotis, Paola Spagnolo, Andrea Francesco Tripodi, Giulio Ubertis, Maria Chiara Ubiali, Inma Valeije Álvarez, Antonio Vallini, Gianluca Varraso, Vito Velluzzi, Paolo Veneziani, John Vervaele, Daniela Vigoni, Costantino Visconti, Javier Wilenmann von Bernath, Francesco Zacchè, Stefano Zirulia

Editore Associazione "Progetto giustizia penale", c/o Università degli Studi di Milano,  
Dipartimento di Scienze Giuridiche "C. Beccaria" - Via Festa del Perdono, 7 - 20122 MILANO - c.f. 97792250157  
ANNO 2025 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.  
Impaginazione a cura di Chiara Pavesi

**Diritto penale contemporaneo – Rivista trimestrale** è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

Il lettore può leggere, condividere, riprodurre, distribuire, stampare, comunicare al pubblico, esporre in pubblico, cercare e segnalare tramite collegamento ipertestuale ogni lavoro pubblicato su "Diritto penale contemporaneo – Rivista trimestrale", con qualsiasi mezzo e formato, per qualsiasi scopo lecito e non commerciale, nei limiti consentiti dalla licenza Creative Commons - Attribuzione - Non commerciale 3.0 Italia (CC BY-NC 3.0 IT), in particolare conservando l'indicazione della fonte, del logo e del formato grafico originale, nonché dell'autore del contributo.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il [Code of Conduct and Best Practice Guidelines for Journal Editors](#) elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies ([clicca qui](#) per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

I contributi da sottoporre alla Rivista possono essere inviati al seguente indirizzo mail: [editor.criminaljusticenetwork@gmail.com](mailto:editor.criminaljusticenetwork@gmail.com). I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali [scaricabili qui](#).

**Diritto penale contemporaneo – Rivista trimestrale** es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación. La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación “Progetto giustizia penale”, con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano*, la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile*.

La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.

El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en “Diritto penale contemporaneo – Rivista trimestrale”, con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons – Attribuzione – Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.

La Revista se puede citar de forma abreviada con el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.

La Revista asume el [Code of Conduct and Best Practice Guidelines for Journal Editors](#) elaborado por el COPE (*Committee on Publication Ethics*).

La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales ([clica aquí](#) para los detalles sobre protección de la privacy y uso de cookies).

Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.

En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.

La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.

La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección [editor.criminaljusticenetwork@gmail.com](mailto:editor.criminaljusticenetwork@gmail.com). Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden [descargar aquí](#)).



**Diritto penale contemporaneo – Rivista trimestrale** is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association “Progetto giustizia penale”, based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

Visitors to the site may share, reproduce, distribute, print, communicate to the public, search and cite using a hyperlink every article published in the journal, in any medium and format, for any legal non-commercial purposes, under the terms of the Creative Commons License - Attribution – Non-commercial 3.0 Italy (CC BY-NC 3.0 IT). The source, logo, original graphic format and authorship must be preserved.

For citation purposes the journal's abbreviated reference format may be used: *DPC-RT*, indicating year of publication and issue.

The journal strictly adheres to the [Code of Conduct and Best Practice Guidelines for Journal Editors](#) drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) ([click here](#) for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication's minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at [editor.criminaljusticenetwork@gmail.com](mailto:editor.criminaljusticenetwork@gmail.com). All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines ([download here](#)).

|                                             |                                                                                                                                                              |     |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| UNIONE EUROPEA<br>E GIUSTIZIA PENALE        | <b>The New Directive 2024/1260 and Confiscation Models in the Fight against Fraud Affecting EU's Financial Interests and Corruption in Comparative Law</b>   | 1   |
| UNIÓN EUROPEA<br>Y JUSTICIA PENAL           | <i>La nuova Direttiva 2024/1260 e i modelli di confisca nella lotta alle frodi che ledono gli interessi finanziari dell'UE e alla corruzione</i>             |     |
| EUROPEAN UNION<br>AND CRIMINAL JUSTICE      | <i>La nueva Directiva 2024/1260 y los modelos de confiscación en la lucha contra el fraude que afecta los intereses financieros de la UE y la corrupción</i> |     |
|                                             | Anna Maria Maugeri                                                                                                                                           |     |
|                                             | <b>AI Act e procedimento penale italiano: una valutazione d'impatto</b>                                                                                      | 88  |
|                                             | <i>El AI Act y los procedimientos penales italianos: una evaluación de impacto</i>                                                                           |     |
|                                             | <i>AI Act and Italian Criminal Proceedings: An Impact Assessment</i>                                                                                         |     |
|                                             | Nicolò Gibelli                                                                                                                                               |     |
| IL DELITTO DI<br>FEMMINICIDIO               | <b>La legge sul femminicidio e le modifiche apportate alla fattispecie dei maltrattamenti</b>                                                                | 116 |
| EL DELITO DE FEMINICIDIO                    | <i>La ley sobre el feminicidio y las modificaciones introducidas en la tipificación del delito de maltrato</i>                                               |     |
| THE CRIME OF FEMICIDE                       | <i>The Law on Femicide and the Changes Made to the Crime of Mistreatment</i>                                                                                 |     |
|                                             | Alessandro Roiati                                                                                                                                            |     |
|                                             | <b>Ancora sul reato di femminicidio: limiti e prospettive di un diritto penale basato sul genere</b>                                                         | 131 |
|                                             | <i>Sobre el delito de feminicidio: límites y perspectivas de un derecho penal basado en el género</i>                                                        |     |
|                                             | <i>On the Crime of Femicide: Limits and Perspectives of a Gender-Based Criminal Law</i>                                                                      |     |
|                                             | Valentina Badalamenti                                                                                                                                        |     |
| RESPONSABILITÀ DA<br>REATO DEGLI ENTI       | <b>La Ley orgánica 5/2024, de 11 de noviembre, del derecho de defensa.</b>                                                                                   | 181 |
| RESPONSABILIDAD PENAL<br>PERSONAS JURÍDICAS | <b>Una lectura desde la perspectiva de las personas jurídicas</b>                                                                                            |     |
| CORPORATE CRIMINAL<br>LIABILITY             | <i>Legge Organica 5/2024, dell'11 novembre, sul Diritto di Difesa.</i>                                                                                       |     |
|                                             | <i>Una lettura dalla prospettiva delle persone giuridiche</i>                                                                                                |     |
|                                             | <i>Organic Law 5/2024, of 11 November, on the Right of Defense.</i>                                                                                          |     |
|                                             | <i>A Reading from the Perspective of Legal Entities</i>                                                                                                      |     |
|                                             | Oliver Pascual Suaña                                                                                                                                         |     |

QUESTIONI

DI DIRITTO PENALE

CUESTIONES

DE DERECHO PENAL

CRIMINAL LAW ISSUES

**Dal dovere di candor del difensore anglosassone alla motivazione confutativa** 197

**del giudice italiano: modelli di accountability ermeneutica a confronto**

*Del deber de candor del defensor anglosajón a la motivación confutativa del juez italiano: comparación entre modelos de accountability hermenéutica*

*From the Anglo-Saxon Defense Attorney's Duty of Candor to the Italian Judge's Rebuttal-Based Reasoning: Comparative Models of Hermeneutic Accountability*

Mario Caterini

**Brevi spunti in tema di determinazione dei limiti temporali di applicabilità** 210

**degli istituti penalistici e processual-penalistici**

*Breves apuntes sobre la determinación de los límites temporales de aplicabilidad de las instituciones de derecho penal sustantivo y procesal*

*Brief Remarks on the Determination of the Temporal Limits of Applicability of Substantive and Procedural Criminal Law Institutions*

Alberto Aimi

**Premialità, rieducazione e giustizia riparativa nei reati di stampo mafioso** 225

*Premialidad, reeducación y justicia restaurativa en los delitos de matriz mafiosa*

*Rewarding, Rehabilitation and Restorative Justice in Mafia Crimes*

Angela Laura Chiodo

**Il complesso rapporto tra esigenze sanzionatorie e valutazione del *pati* del reo** 251

*La compleja relación entre las exigencias sancionadoras y la valoración del sufrimiento del infractor*

*The Complex Relationship Between Sanctioning Requirements and Assessment of the Offender's Suffering*

Andrea Fortunato

UNIONE EUROPEA E GIUSTIZIA PENALE  
*UNIÓN EUROPEA Y JUSTICIA PENAL*  
*EUROPEAN UNION AND CRIMINAL JUSTICE*

- 1    **The New Directive 2024/1260 and Confiscation Models in the Fight against Fraud Affecting EU's Financial Interests and Corruption in Comparative Law**  
*La nuova Direttiva 2024/1260 e i modelli di confisca nella lotta alle frodi che ledono gli interessi finanziari dell'UE e alla corruzione*  
*La nueva Directiva 2024/1260 y los modelos de confiscación en la lucha contra el fraude que afecta los intereses financieros de la UE y la corrupción*  
Anna Maria Maugeri
- 88    **AI Act e procedimento penale italiano: una valutazione d'impatto**  
*El AI Act y los procedimientos penales italianos: una evaluación de impacto*  
*AI Act and Italian Criminal Proceedings: An Impact Assessment*  
Nicolò Gibelli

# *AI Act e procedimento penale italiano: una valutazione d'impatto\**

## *El AI Act y el procedimiento penal italiano: una evaluación de impacto*

## *AI Act and Italian Criminal Proceedings: An Impact Assessment*

NICOLÒ GIBELLI

*Dottorando di ricerca in procedura penale presso le Università di Bologna e Pisa  
nicolo.gibelli2@unibo.it*

INTELLIGENZA ARTIFICIALE,  
DIRITTI PROCESSUALI  
FONDAMENTALI

INTELIGENCIA ARTIFICIAL,  
DERECHOS PROCESALES  
FUNDAMENTALES

ARTIFICIAL INTELLIGENCE,  
FUNDAMENTAL PROCEDURAL RIGHTS

### ABSTRACTS

Il contributo esamina le implicazioni che l'approvazione del regolamento (UE) 2024/1689 in materia di intelligenza artificiale (*AI Act*) avrà sul procedimento penale italiano. Nel contesto investigativo già da tempo si riscontra l'impiego di diverse IA, utili soprattutto all'identificazione della persona sottoposta a indagini, ma anche a ottimizzare analisi scientifiche o prevedere il verificarsi di futuri eventi criminosi. Il lavoro si propone, innanzitutto, di sistematizzare gli usi noti dell'IA nel procedimento penale, distinguendo tra i sistemi impiegati per la prevenzione del crimine, per le indagini e a supporto del giudice. Valuta, poi, l'impatto dell'*AI Act* sul futuro di queste tecnologie in Italia, verificando quando il loro impiego risulti consentito, quando ammesso entro determinati limiti e quando vietato. L'obiettivo è dunque fornire all'operatore del processo italiano una guida sistematica alle nuove intelligenze artificiali.

El artículo examina las implicaciones que tendrá la aprobación del Reglamento (UE) 2024/1689 sobre inteligencia artificial (*AI Act*) en el procedimiento penal italiano. En el contexto investigativo, desde hace tiempo se constata el empleo de diversas herramientas de IA, útiles sobre todo para la identificación de las personas sometidas a investigación, pero también para optimizar los análisis científicos o predecir la ocurrencia de futuros delitos. El objetivo principal de este trabajo es sistematizar los usos conocidos de la IA en el procedimiento penal, distinguiendo entre los sistemas utilizados para la prevención del delito, la investigación y el apoyo judicial. Al mismo tiempo, evalúa el impacto del *AI Act* sobre el futuro de estas tecnologías en Italia, verificando cuándo se permite su uso, cuándo se admite dentro de determinados límites, y cuándo está prohibido. El objetivo es, por tanto, proporcionar a los operadores del procedimiento penal italiano una guía sistemática sobre las nuevas tecnologías de inteligencia artificial.

\* Desidero rivolgere un sentito ringraziamento al mio Maestro, il Professor Michele Caianiello, per il suo indispensabile contributo alle riflessioni contenute nel presente lavoro.

This paper examines the implications that the approval of Regulation (EU) 2024/1689 on artificial intelligence (AI Act) will have on Italian criminal proceedings. In the investigative context, various forms of AI have been already deployed, mainly to identify persons under investigation, but also to optimize scientific analysis or predict future criminal events. This work aims, first of all, to systematize the known uses of AI in criminal proceedings, distinguishing between systems used for crime prevention, investigation, and judicial support. At the same time, it assesses the impact of the AI Act on the future of these technologies, verifying when their use is permitted, when it is allowed within certain limits, and when it is prohibited. The aim is therefore to provide Italian legal practitioners with a systematic guide to new artificial intelligence technologies.

## SOMMARIO

1. Introduzione. – 2. La regolamentazione dell'AIA: cinque criticità. – 3. L'IA come strumento di prevenzione. – 3.1. I sistemi di polizia predittiva (*predictive policing*). – 3.1.1. La polizia predittiva in generale. – 3.1.2. I sistemi di polizia predittiva in Italia. – 3.2. Sistemi biometrici per l'identificazione da remoto in pubblico e in *real time*. – 3.2.1. L'identificazione remota preventiva in generale e nell'*AI Act*. – 3.2.2. Il versante interno. Il S.A.R.I. *Real time* alla ricerca di una base giuridica. – 4. L'IA come mezzo d'investigazione e di prova. – 4.1. Sistemi biometrici per l'identificazione da remoto, ma non in *real time*. – 4.1.1. Generalità. La regolamentazione europea dell'identificazione remota differita. – 4.1.2. I risvolti sull'impiego del S.A.R.I. *Enterprise* durante le indagini e sull'utilizzabilità processuale dei risultati. – 4.2. Sistemi biometrici impiegati per l'identificazione, ma non da remoto. – 4.3. Sistemi biometrici impiegati per scopi diversi dall'identificazione. – 4.4. Sistemi non biometrici a uso investigativo e probatorio. – 4.5. Sistemi per il calcolo del rischio di recidiva (*risk assessment tools*). – 4.5.1. La valutazione automatica dei precedenti dell'imputato: generalità. – 4.5.2. *Risk assessment tools* nel diritto nazionale. – 5. L'IA come mero supporto del giudice e delle parti. – 6. Riflessioni conclusive.

## 1.

## Introduzione.

Il 2 agosto 2024 è entrato in vigore il regolamento 2024/1689 del Parlamento europeo e del Consiglio, noto come *AI Act* (d'ora in avanti "AIA" o il "regolamento"), che stabilisce regole armonizzate per l'impiego dell'intelligenza artificiale ("IA", anche inteso, forse più correttamente,<sup>1</sup> al plurale) nell'Unione Europea.

Il regolamento era chiamato a disciplinare una vera e propria rivoluzione tecnologico-sociale: solo per fare un esempio, se alla data della prima proposta della Commissione (21 aprile 2021) *ChatGPT* non era ancora stato rilasciato,<sup>2</sup> neanche quattro anni dopo, quando i primi capi del regolamento sono divenuti applicabili (2 febbraio 2025, v. art. 113 AIA) il *Generative Pre-trained Transformer* di *OpenAI* contava già 400 milioni di utenti settimanali nel mondo.<sup>3</sup> Sono contemporaneamente nate le prime imprese "*AI-first*", che preferiscono le IA ai lavoratori umani.<sup>4</sup> Intanto, nelle sale operatorie, *software* diagnostici aiutano i medici umani nel distinguere le forme tumorali da quelle benigne.<sup>5</sup>

Il regolamento – già iconicamente rinominato «Costituzione europea sull'Intelligenza Artificiale»<sup>6</sup> – asseconda questa incipiente rivoluzione, tentando al contempo di salvaguardare la salute e la sicurezza delle persone fisiche, ma anche taluni diritti delle persone giuridiche (specialmente in materia di proprietà intellettuale). Dal canto suo, il legislatore italiano, con la l. n. 132/2025 ha già assorbito i principi fondamentali del regolamento, dettato alcune linee di indirizzo generali per l'implementazione dei nuovi *tools* e, soprattutto, delegato il Governo ad adottare una «disciplina organica relativa all'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale» in conformità con il mutato assetto normativo (art. 8, c. I, l. cit.).

Delle molteplici ricadute che il regolamento avrà sull'utilizzo delle IA in Europa, il presente lavoro si propone di analizzare quelle che interesseranno il procedimento penale italiano. Le IA si sono infatti già integrate nella normalità investigativa e processuale, che hanno promesso di rivoluzionare tagliandone alcune inefficienze. Esse oggi catalizzano indagini e prove: per accennare a qualche esempio, algoritmi comparativi per l'analisi delle immagini migliorano i riconoscimenti; *software* di IA completano le indagini genetiche con accurate distribuzioni statistiche; il *machine learning* ricostruisce la probabile traiettoria di oggetti come automobili o proiettili.

Si prospetta, quindi, un poderoso miglioramento dell'efficienza investigativa, grazie alla disponibilità di una potenza di calcolo tecnicamente "inumana". Ed è proprio l'inumanità – nel suo significato aristotelico di manifestazione di ingiustizia<sup>7</sup> – a serbare il rischio più marcato

<sup>1</sup> Come noto si tratta di una famiglia di tecnologie multiforme e in continua evoluzione, v. in generale FLORIDI (2014); v. anche BENANTI (2024).

<sup>2</sup> V. *Presentazione di ChatGPT*, disponibile sul [sito di Open AI](#), 30 novembre 2022.

<sup>3</sup> V. ad es. *OpenAI's weekly active users surpass 400 million*, in *Reuters*, 20 febbraio 2025.

<sup>4</sup> *AI first, come l'approccio che mette l'intelligenza artificiale al centro sta cambiando le aziende. E il lavoro*, in *Wired.it*, 30 aprile 2025.

<sup>5</sup> Per gli usi clinici dell'IA v. CALIGIORE (2024).

<sup>6</sup> NOVELLI (2024).

<sup>7</sup> Il riferimento è al celebre passo sulla giustizia dell'Etica Nicomachea, Libro V, per cui si rimanda a quest'opera nella versione curata da MAZZARELLI (2000).

per il processo penale, ovvero quello di un lento allontanamento dalle garanzie procedurali tradizionali, prima fra tutte il contraddittorio nella formazione della prova,<sup>8</sup> ma anche la tutela della riservatezza e della presunzione di non colpevolezza. Garanzie di solida base costituzionale che l'AIA era chiamato a tutelare, assicurandosi che le IA fossero sottoposte al primato dei principi di diritto in luogo di qualsiasi altro tipo di normatività.<sup>9</sup>

In questa sede non ci si propone di valutare il risultato ottenuto dal regolamento attraverso una sua analisi sistematica, quanto piuttosto con un confronto tra lo stato di fatto delle IA processualpenalistiche italiane e il nuovo quadro normativo europeo. In virtù di questa scelta di campo, ad esempio, si è ritenuto di distinguere – là dove il regolamento tace – tra le singole fasi del procedimento penale italiano e di descrivere, nell'alveo di ciascuna di esse, gli impieghi attuali delle IA, nonché le futuribili conseguenze dell'approvazione del regolamento.

Questa operazione non è priva di rischi: le categorie del diritto interno non sono sempre sovrapponibili a quelle del diritto europeo, e il parallelismo può generare approssimazioni e storture. Tuttavia, il tentativo sembra utile: la lettura meramente analitica dell'AIA ne svilirebbe la portata innovativa, come se il regolamento non fosse in grado di misurarsi con le dinamiche effettive dei processi penali nazionali.

Il presente studio è organizzato in una premessa di carattere generale e in una seconda parte, per così dire, “speciale”. Nella premessa si condurrà una riflessione sulle tecniche di normazione adottate dall'AIA nel campo della giustizia penale (par. 2). Dalla lettura del regolamento, infatti, emerge immediatamente come il legislatore europeo sia ricorso a una serie di regole ed eccezioni, prevedendo per le c.d. «attività di contrasto»<sup>10</sup> numerose deroghe al regime valevole in generale per le altre IA. L'avvicinarsi di disposizioni ordinarie e derogatorie in campo processualpenalistico è una vera e propria chiave di lettura del regolamento e serve da guida per comprendere a fondo le implicazioni che le nuove disposizioni avranno sulle IA oggi operanti sul territorio nazionale.

Nella parte “speciale”, invece, si tenterà una ricognizione sistematica degli usi noti dell'IA nelle attività di contrasto, distinguendo tre aree fondamentali: la prevenzione (par. 3), l'investigazione e la prova (par. 4) e il supporto materiale (par. 5). Per ogni categoria, ove rilevante, il contributo dapprima descriverà generalmente il sistema esaminato e il suo statuto di derivazione europea; successivamente lo analizzerà nello specifico contesto dell'ordinamento italiano.

## 2.

### La regolamentazione dell'AIA: cinque criticità.

Come ormai noto, il regolamento individua quattro categorie di rischio –inaccettabile, elevato, limitato e minimo – sulla base della potenziale incidenza dell'IA su diritti fondamentali e interessi giuridicamente rilevanti.<sup>11</sup> La classificazione consente di modulare l'invasività degli obblighi di conformità tecnica e documentale in modo proporzionato al grado di rischio.

In termini applicativi, gli adempimenti imposti dall'AIA a sviluppatori e *deployer* presentano significative analogie con quelli delineati dal regolamento 2016/679 (c.d. *G.D.P.R.*). Si tratta, in sintesi, di un sistema di *compliance* integrato, sulla cui efficacia dissuasiva la dottrina ha già espresso più di un dubbio.<sup>12</sup>

Al vertice della “piramide del rischio” si trovano le IA che presentano un rischio inaccettabile. L'art. 5 AIA (almeno nominalmente) le vieta: è impossibile conciliarne l'uso con la protezione dei diritti fondamentali degli individui. In questa categoria il regolamento colloca, ad esempio, le IA impiegate per il riconoscimento facciale e usate per finalità di contrasto, ma solo se il sistema opera in *real time* in luoghi aperti al pubblico (v. *infra*).

Subito al di sotto dei sistemi a rischio inaccettabile si annoverano quelli ad alto rischio. Per quanto qui interessa, vi rientrano le IA operanti negli ambiti elencati in un allegato del regolamento, il terzo. Ad esempio, la biometria (all. III, n. 1), le attività di contrasto (all. III, n. 6)

<sup>8</sup> FERRUA (2024), p. 20.

<sup>9</sup> GALGANI (2020), p. 82.

<sup>10</sup> Cioè quelle svolte dalle autorità di contrasto o per loro conto ai fine di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali (art. 3, n. 46 AIA).

<sup>11</sup> Per una visione, anche critica, dell'approccio del regolamento, cfr. NOVELLI ET AL. (2024). Più in generale, sul tema, cfr. DONATI (2025); MARCHETTI (2024); CASONATO E MARCHETTI (2021).

<sup>12</sup> QUATTROCOLO (2025), p. 11, paragonando gli obblighi di cui all'AIA al d.lgs. 231/2001 in materia di responsabilità amministrativa degli enti.

o l'amministrazione della giustizia (all. III, n. 8). Per poter essere commercializzati e utilizzati tali modelli di IA devono necessariamente conformarsi a stringenti requisiti,<sup>13</sup> che corrispondono a obblighi ripartiti tra i diversi attori della catena di valore dell'IA (capo III, sez. 3 AIA).

Seppure i vincoli imposti ai sistemi ad alto rischio siano concepiti per trovare un'applicazione generale, si riconosce immediatamente l'esistenza di un "doppio binario" in cui le IA impiegate nelle attività di contrasto subiscono un trattamento in larga parte derogatorio.

L'approccio appare ragionevole, poiché il mantenimento di requisiti troppo rigidi per l'uso delle IA penalistiche avrebbe potuto ostacolare la portata innovativa di sistemi utili per la prevenzione e il perseguimento dei reati.

Per quanto corretta nelle intenzioni, però, questa tecnica legislativa ha causato qualche distorsione. Da un punto di vista metodologico, di certo il costante susseguirsi di eccezioni non facilita la lettura del regolamento, che in alcuni passaggi non chiarisce cosa sia permesso e cosa, invece, vietato. Quanto al merito, il regolamento eccede nel sottoporre le attività di contrasto a una disciplina derogatoria, intervenendo con distinzioni *ad hoc* quando sarebbe stato meglio non intervenire, o, viceversa, non differenziando in casi che lo avrebbero meritato. Sono in particolare cinque le criticità da evidenziare.

La più importante è la limitazione dell'ambito oggettivo di applicazione del regolamento, il quale non copre i sistemi utilizzati (in via esclusiva) «per scopi militari, di difesa o di sicurezza nazionale», indipendentemente dal tipo di entità che li impieghi (art. 2, par. 3 AIA). La vistosa eccezione parrebbe essere stata desiderata fortemente dai negoziatori d'oltralpe, cui i nostri si sarebbero ben presto accodati.<sup>14</sup> Comunque, è evidente che la formula della sicurezza nazionale — come il *pitthos* di Pandora — è tanto vaga da poter giustificare, all'occorrenza, quasi ogni deroga all'applicazione del regolamento *tout court*. Opportunamente, la recente legge italiana in materia di intelligenza artificiale (art. 6, c. I, l. 23 settembre 2025, n. 132) riduce la portata dell'eccezione, indicando con precisione i casi di deroga. Ad esempio, quando a utilizzare l'IA sono le forze di polizia ai fini della sicurezza nazionale, l'applicazione alla legge italiana è esclusa solo se le attività sono dirette a prevenire e contrastare specifici gravi reati.<sup>15</sup>

Una seconda criticità si pone per la valutazione di conformità delle IA ad alto rischio con i requisiti imposti dal regolamento (art. 43 AIA).<sup>16</sup> Per tutti questi sistemi (quindi inclusi quelli penalistici) basta in via di principio un mero controllo interno (art. 43 AIA, paragrafi 1 e 2), invece di un regime autorizzatorio affidato ad autorità pubbliche.<sup>17</sup> Nei (pochi) casi in cui serve un controllo esterno, peraltro, a fungere da organismo notificato è la *market surveillance authority*, che nell'ordinamento italiano è un'agenzia governativa.<sup>18</sup>

In terzo luogo, desta perplessità l'obbligo di registrazione dei sistemi ad alto rischio usati nelle attività di contrasto in una sezione non pubblica del *database* europeo (art. 49, par. 4 AIA). L'AIA ha infatti previsto l'obbligo di previa registrazione di tutte le IA ad alto rischio di cui all'allegato III in una banca dati europea, nella quale andranno inseriti importanti dati relativi al funzionamento e all'allenamento del sistema, nonché una copia della dichiarazione di conformità e delle istruzioni d'uso (all. VIII, lett. a) e 71 AIA). Di regola, tali informazioni sono accessibili al pubblico (art. 71, par. 4 AIA). Ma ai *software* di polizia s'impone riservatezza: finiscono in una lista segreta e le informazioni da registrare sono limitate. Ad esempio, non saranno ostese le metriche di robustezza e cybersicurezza del sistema (art. 13 AIA).

V'è poi un quarto profilo critico, ovvero la previsione di esenzioni dagli obblighi di trasparenza che vincolano fornitori e *deployers* di determinate IA (art. 50 AIA). In genere, le persone

<sup>13</sup> Dalla conformità a standard tecnici stabiliti dal regolamento (art. 8 AIA) all'implementazione di un sistema di gestione del rischio (art. 9 AIA); dall'utilizzo di dati pertinenti, rappresentativi, privi di errori e completi per l'addestramento (art. 10 AIA) alla redazione di una documentazione tecnica dettagliata (art. 11 AIA); dal tracciamento gli «eventi» (c.d. log: art. 12 AIA) alla preparazione di informative sul funzionamento del sistema (art. 13 AIA); dall'implementazione di misure che consentano una supervisione umana efficace (art. 14 AIA) alla garanzia di un elevato livello di accuratezza, robustezza e sicurezza informatica (art. 15 AIA).

<sup>14</sup> *France spearheads member state campaign to dilute European Artificial Intelligence regulation*, in *Investigate Europe*, 3 novembre 2023.

<sup>15</sup> Si tratta dei reati di cui all'art. 9, comma I, lettere b) e b-ter) della l. 16 marzo 2006, n. 146, relativa alle operazioni sotto copertura. In tutti gli altri casi, dunque (e ad eccezione di alcune deroghe relative alle attività delle Agenzie di *intelligence*), il perseguimento di finalità di sicurezza nazionale da parte delle forze di polizia non dovrebbe consentire di aggirare la disciplina interna.

<sup>16</sup> In generale, il *conformity assessment* imposto dal regolamento può essere effettuato sulla base di un mero controllo interno (all. VI) o attraverso una (più rigorosa) valutazione compiuta da un «organismo notificato» (all. VII), cioè un'organizzazione terza, obiettiva e indipendente a ciò deputata (art. 43 AIA).

<sup>17</sup> Sul punto, v. MARCHETTI (2024), p. 8.

<sup>18</sup> V'è da notare che la Commissione, nel suo parere circostanziato n. C (2024)7814 aveva rilevato che le autorità di governance nominate dall'Italia – AgID (Agenzia per l'Italia Digitale) e ACN (Agenzia per la Cybersicurezza Nazionale) – sono autorità governative che non possono assicurare piena indipendenza. Tali autorità sono state poste al vertice del sistema di *governance* nazionale dall'art. 20 l. 132/2025.

fisiche debbono essere informate del fatto che vi sono esposte: ad esempio, devono poter riconoscere di stare interagendo con una IA, salvo che ciò sia evidente (art. 51, par. 1 AIA). Oneri analoghi si estendono alle IA generative, ai sistemi di riconoscimento delle emozioni e di categorizzazione biometrica, nonché alla generazione e manipolazione di *deep fakes* e alla produzione di testi (art. 51, parr. 2, 3, 4 AIA). Tuttavia, un'eccezione "in serie" esenta dall'obbligo di informativa i sistemi «autorizzati dalla legge ad accertare, prevenire, indagare o perseguire reati». Non si capisce, in tutta franchezza, il senso di tale eccezione. Anche le IA impiegate nelle attività di contrasto – forse soprattutto queste ultime – dovrebbero essere tenute a un simile, basilare adempimento.

Infine, si deve porre l'attenzione sull'impossibilità di accedere direttamente al codice sorgente dei programmi utilizzati nei procedimenti penali. L'AIA non garantisce alcun diritto di accesso diretto al *source code* da parte dei soggetti coinvolti da decisioni che hanno comportato l'utilizzo di IA. Piuttosto, il regolamento individua un intermediario, la *market surveillance authority*,<sup>19</sup> cui gli interessati possono rivolgere richiesta motivata di accesso. Tuttavia, solo l'autorità competente (e non il singolo richiedente) potrà prenderne visione al ricorrere di specifiche condizioni (art. 74, par. 13 AIA).<sup>20</sup> In generale, invece, prevale l'obbligo di segretezza per tutte le informazioni relative al sistema, incluso il codice sorgente (art. 78 AIA). Qui, forse, è mancato il coraggio di subordinare la tutela dei diritti di proprietà intellettuale al supremo valore della libertà personale, e quindi di garantire il diritto a un controllo più approfondito del sistema da parte dei soggetti direttamente lesi dalla decisione algoritmica.<sup>21</sup>

### 3. L'IA come strumento di prevenzione.

Tanto premesso in via generale, si procederà ora con una rassegna sistematica degli usi delle IA nelle varie fasi del procedimento penale, seguendo la scansione della procedura italiana.

A catalizzare le attenzioni durante la negoziazione dell'AIA è stato certamente l'impiego delle IA nella fase preventiva: qui gli algoritmi, integrandosi con le tradizionali tecniche di *intelligence*, possono contribuire a identificare situazioni di rischio in ottica di prevenzione del crimine. Non richiedendo la previa commissione di un reato, l'attivazione di queste IA pone evidentemente interrogativi in tema di bilanciamento tra l'efficienza nella prevenzione dell'illegalità e il diritto alla *privacy*.<sup>22</sup>

In questa sede si darà conto di due categorie di *software*, rilevanti per il nostro ordinamento in quanto già impiegate ovvero in via di implementazione:

Sistemi di polizia predittiva (*predictive policing*, 3.1);

Sistemi biometrici per l'identificazione da remoto in pubblico e in *real time* (3.2)

#### 3.1. I sistemi di polizia predittiva (*predictive policing*).

##### 3.1.1. La polizia predittiva in generale.

Con la medesima espressione *predictive policing* si fa riferimento a due categorie concettualmente distinte di *software* per la prevenzione del crimine. La prima è rappresentata dai c.d. sistemi *place-based*, i quali operano attraverso l'analisi di dati eterogenei — non solo di natura strettamente criminologica, ma anche ambientale, urbanistica e socioeconomica — al fine di

<sup>19</sup> A norma dell'art. 74(8) del regolamento, per i sistemi ad alto rischio elencati nell'allegato III, punto 1, nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e per i sistemi ad alto rischio di cui ai punti 6, 7 e 8 del medesimo allegato, gli Stati membri designano come autorità di vigilanza del mercato ai fini del regolamento le autorità di controllo competenti per la protezione dei dati a norma del regolamento (UE) 2016/679 o della direttiva (UE) 2016/680 o qualsiasi altra autorità designata a norma delle stesse condizioni di cui agli articoli da 41 a 44 della direttiva (UE) 2016/680.

<sup>20</sup> Ecco le condizioni: a) l'accesso al codice sorgente è necessario per valutare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo III, sezione 2; e b) le procedure di prova o di *audit* e le verifiche basate sui dati e sulla documentazione presentati dal fornitore sono state esaurite o si sono dimostrate insufficienti.

<sup>21</sup> Sulla relazione tra *trade secrets* e IA v. QUATTROCOLO (2020), pp. 93 ss.; CHESSMAN (2017), pp. 209 ss.

<sup>22</sup> *Facial recognition technology: fundamental rights considerations in the context of law enforcement, Report FRA – European Union Agency for Fundamental Rights*, 27 novembre 2019.

individuare le aree geografiche a maggiore probabilità di verifica di eventi delittuosi.<sup>23</sup> Il risultato del calcolo è una “mappa di rischio”, in cui le zone “calde” sono evidenziate da colori più intensi. I sistemi *place-based* non forniscono, dunque, accertamenti: si limitano a generare *investigative leads*, spunti investigativi privi di valenza probatoria, destinati semplicemente a guidare l’attività preventiva della polizia senza vincolarne l’esito.

Accanto a questi si menzionano comunemente i sistemi c.d. *person-based* o *individual-based*,<sup>24</sup> che, partendo da elementi comuni tra crimini compiuti in serie (ad es.: ora, data, luogo, tipo di attività, tipo di reato, età del sospettato per come percepita dai testimoni, altezza, struttura corporea, colore della pelle, dei capelli, degli occhi,...) predicono un ipotetico profilo personologico dell’autore dei delitti (ad es. un *serial killer*).<sup>25</sup> Anche i sistemi *person-based* sono utilizzati unicamente nella fase delle indagini allo scopo di fornire spunti investigativi, ma, a differenza di quelli *place-based*, essi si basano sulla profilazione.<sup>26</sup> Diversamente dai *risk assessment tools*, inoltre, non si propongono di valutare il rischio di recidiva in soggetti già coinvolti nel procedimento, quanto piuttosto di orientare le indagini verso profili personologici ritenuti statisticamente compatibili con la sequenza dei fatti oggetto di analisi.<sup>27</sup>

L’AIA non definisce né nomina i *predictive policing tools*, nemmeno tra i sistemi ad alto rischio, e da ciò dovrebbe inferirsi una loro totale liberalizzazione.<sup>28</sup> Tuttavia, come appena accennato, alcuni di questi programmi svolgono attività di profilazione in senso tecnico. L’allegato III, n. 6, lett. e) AIA classifica come ad alto rischio i sistemi impiegati per effettuare la profilazione di persone fisiche «nel corso dell’indagine, dell’accertamento e del perseguimento di reati». Quindi, nel caso in cui un sistema di *predictive policing* venisse utilizzato ai fini della profilazione in fase di indagini,<sup>29</sup> esso dovrebbe rispettare gli obblighi di *compliance* concepiti per le IA ad alto rischio.

### 3.1.2. *I sistemi di polizia predittiva in Italia.*

La distinzione tra sistemi che effettuano profilazione e quelli che ne prescindono riverbera la sua eco anche nell’ordinamento italiano.

Sul versante interno, è da anni attivo il sistema di polizia predittiva *place-based XLaw*, oggetto di sperimentazione da diverse Questure sul territorio nazionale. Le mappe di *XLaw* associano al rischio-reato colori via via più intensi, sempre secondo metriche probabilistiche.<sup>30</sup>

La Questura di Milano ha testato anche un *software person-based*, destando peraltro l’interesse del Ministero dell’Interno.<sup>31</sup> Il programma, sviluppato nel contesto del progetto “Giove” (già *KeyCrime*), restituisce il potenziale profilo personologico dell’autore di un crimine seriale basandosi su una serie di dati noti (anche personali). L’approccio di Giove sembra dunque «marcatamente più invasivo»<sup>32</sup> di *XLaw*.

Ora, il regolamento, come si è già visto, non sembra frapporre alcun divieto all’impiego di *software* di polizia predittiva negli Stati membri.<sup>33</sup> Solamente ove gli stessi vengano impiegati a fini della profilazione (come Giove) finiranno per ricadere tra i sistemi ad alto rischio per via dell’estensione operata dall’all. III, n. 6, lett. e) AIA.

<sup>23</sup> V., in generale, PIETROCARLO (2024), GARRETT (2023), UCHIDA (2009), e *AI and policing: the benefits and challenges of artificial intelligence for law enforcement*, Europol Report del 23 settembre 2024, p. 15.

<sup>24</sup> *AI and policing: the benefits and challenges*, cit., p. 15.

<sup>25</sup> Intervista a Elia Lombardo sulla polizia predittiva, *XLAW* e *KeyCrime* riflessioni, in *Rivista.AI*, 18 ottobre 2024.

<sup>26</sup> Il concetto di profilazione è definito dall’art. 4 reg. 2016/679 (G.D.P.R.) come qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l’affidabilità, il comportamento, l’ubicazione o gli spostamenti di detta persona fisica.

<sup>27</sup> QUATTROCOLO (2021b), p. 261.

<sup>28</sup> Nonostante la totale assenza di regolamentazione, tuttavia, parte della dottrina ha ritenuto di leggere nel divieto relativo ai *risk assessment tools* (art. 5(1)(d) AIA) anche un divieto di uso e commercializzazione degli strumenti di *predictive policing*. Riferisce questa posizione QUATTROCOLO (2025), p. 4. Correttamente l’Autrice sostiene che il riferimento normativo sia ai sistemi di *risk assessment*.

<sup>29</sup> Non, quindi, in fase preventiva. Tuttavia, nel peculiare contesto delle indagini relative a crimini seriali — ambito d’elezione dei sistemi qui considerati — le fasi investigativa e preventiva tendono fisiologicamente a sovrapporsi, rendendo incerta la delimitazione tra ciò che è escluso e ciò che ricade nel perimetro dell’AIA.

<sup>30</sup> In tema, v. CONTISSA ET AL. (2019), pp. 619 ss.; GIALUZ E QUATTROCOLO (2023).

<sup>31</sup> ESPOSITO (2024).

<sup>32</sup> Intervista a Elia Lombardo sulla Polizia Predittiva, *XLAW* e *KeyCrime* riflessioni, cit.

<sup>33</sup> Eppure, nelle more dell’approvazione dell’AIA, le incertezze definitorie avevano persino portato l’ideatore di *KeyCrime* a mettere la start-up in liquidazione. Cfr. *Perché la più avanzata startup italiana di polizia predittiva è sull’orlo del baratro*, in *Wired Italia*, 31 gennaio 2024.

Inoltre, va ricordato che, nell'ambito delle attività di polizia, sono proibite le decisioni basate «unicamente» sul processamento automatizzato di dati che incidano negativamente sugli individui, a meno che non siano autorizzate dal diritto dell'Unione o da quello degli Stati membri e sempre salve le garanzie adeguate per i diritti e le libertà dell'interessato (art. 11 direttiva 2016/680). Tra queste deve essere garantito almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento (v. *semper* art. 11 direttiva cit.). Ne consegue che il *predictive policing* dovrebbe considerarsi vietato ove manchi di una (ri)valutazione umana.<sup>34</sup>

La limitazione, tuttavia, non sembra particolarmente stringente. Per un verso, essa è facilmente aggirabile, perché con un minimo coinvolgimento umano nelle decisioni algoritmiche queste non saranno più «unicamente» basate sul processamento automatizzato di dati. Quindi, non varrà più il divieto. Sotto un altro profilo, la garanzia del controllo umano rischia di non essere particolarmente efficace, dovendosi pronosticare che il controllore, non potendo entrare nel merito della valutazione algoritmica, finirà per appiattirvisi, salvo errori macroscopici.<sup>35</sup>

## 3.2. *Sistemi biometrici per l'identificazione da remoto in pubblico e in real time.*

### 3.2.1. *L'identificazione remota preventiva in generale e nell'AI Act.*

L'AIA regola l'identificazione biometrica remota attraverso un "doppio binario" che si dipana attraverso due modalità di utilizzo di queste IA.

Da un lato vi è un binario "garantito", laddove l'identificazione avvenga da remoto, in *real time*, in spazi accessibili al pubblico e per finalità di contrasto. In tali casi l'uso dell'IA è in linea di principio vietato, salva la ricorrenza di talune ben specificate eccezioni e il rispetto di talune garanzie. In tutti gli altri casi — anche qualora manchi uno solo dei requisiti appena richiamati — il sistema rientrerà nell'alveo di quelli ad alto rischio, e sarà dunque soggetto al relativo regime, senza incorrere nel divieto.

Per delineare con esattezza il perimetro di questa distinzione, dalla quale discendono conseguenze giuridiche di non poco conto, è opportuno ricostruire la nozione di identificazione biometrica remota in tempo reale in luoghi aperti al pubblico, ovvero gli elementi della definizione che instradano sul primo dei "binari" menzionati.

Innanzitutto, occorre intendersi sul concetto di identificazione biometrica. L'AIA la definisce come il «riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati» (art. 3, n. 35) AIA). Non è identificazione biometrica, ad esempio, la mera verifica di un volto operata da un *device*, perché in quel caso non si ricerca attivamente l'identità di una persona.<sup>36</sup>

Il considerando n. 15 AIA si preoccupa di menzionare le singole "risorse biometriche" sfruttabili per la determinazione dell'identità. Non c'è solo il volto: la lista comprende anche il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, e, generalmente, «altre caratteristiche». Tra queste ve ne sono di comparabili da remoto, cioè senza il coinvolgimento attivo della persona sottoposta all'identificazione, e altre che, invece, presuppongono necessariamente una collaborazione dell'identificando.

Il divieto di cui all'art. 5 AIA scatta solo nel primo caso.<sup>37</sup> Evidentemente, il pensiero va subito ai sistemi di identificazione facciale (*face identification*): rispetto ad altri metodi di

<sup>34</sup> SUNDE (2022), pp. 29 ss.

<sup>35</sup> CONTISSA ET AL. (2019), p. 629.

<sup>36</sup> Per una descrizione dettagliata si rimanda a SACCHETTO (2023), pp. 243 e ss. Diversa è la verifica facciale (*face verification*), con cui si comparano due immagini note per verificare se vi sia ritratta la medesima persona. Ad esempio, lo sblocco di molti odierni *smartphone* si basa sul confronto tra l'immagine del volto del proprietario, impostata come parametro, e quella della persona che sta tentando di accedere al cellulare. I sistemi utilizzati per la mera verifica sono perfino esclusi dai sistemi ad alto rischio di cui all'allegato III, cfr. all. III, n. 1, lett. a) AIA. V. anche ANNEX to the Communication to the Commission on the Approval of the content of the draft Communication from the Commission – Commission guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), p. 98.

<sup>37</sup> Informare semplicemente le persone della presenza di telecamere non vale a determinarne un loro coinvolgimento attivo, cfr. *Commission guidelines*, cit., p. 99.

riconoscimento biometrici essi sono infatti suscettibili di estesa applicazione.<sup>38</sup> Lo stesso si potrebbe dire per i sistemi basati sull'analisi della voce o dell'andatura.<sup>39</sup>

Ancora, per ricadere nel divieto, l'attività deve avvenire in *real time*: il requisito è definito come «assenza di ritardi significativi», con tutte le incertezze del caso. Sul punto, le linee guida della Commissione propongono il seguente criterio: manca un ritardo significativo se e in quanto gli identificandi sono ancora presenti sul luogo di reperimento del dato biometrico.<sup>40</sup> Così un'IA che effettui riconoscimenti durante l'ingresso degli spettatori a un concerto in uno stadio opererebbe in *real time* (utilizzo vietato); ma se, successivamente al concerto, e quindi una volta che gli spettatori hanno lasciato lo stadio, si utilizzasse l'IA per identificare volti nelle immagini video precedentemente ottenute, il ritardo sarebbe significativo e il riconoscimento, dunque, *ex post*: l'identificazione torna lecita.<sup>41</sup>

Da ultimo, si richiede che il sistema di identificazione biometrica remota in *real time* sia usato in luoghi aperti al pubblico. Non sono tali, evidentemente, gli spazi destinati a permettere l'ingresso solo di determinate persone (come i luoghi di lavoro). Lo sono, invece, i mezzi pubblici e i teatri, perché la presenza di condizioni di accesso (come un biglietto o un titolo di viaggio) non vale ad escludere la pubblicità di un luogo, secondo la definizione dello stesso AIA.<sup>42</sup> È evidente che rimane una zona grigia legata all'interpretazione del concetto di «condizioni di accesso», ma un minimo di incertezza sembrerebbe inevitabile.

Superato questo imbuto definitorio, potrà finalmente operare il divieto generale di utilizzo dei sistemi di identificazione biometrica da remoto di cui all'art. 5, par. 1, lett. h) AIA.

Tuttavia, la fatica per giungere all'applicazione del divieto è mal ripagata. Si tratta, infatti, di un'interdizione solo apparente, che viene meno qualora l'identificazione risulti «strettamente necessaria» per il perseguimento di obiettivi specificamente tipizzati dal regolamento. Tra questi: la ricerca di vittime vulnerabili o scomparse, la prevenzione di minacce gravi e imminenti per la vita o l'incolumità delle persone, o ancora l'identificazione di soggetti sospettati di gravi reati, elencati nell'allegato II.

Le eccezioni, come si vede, sono estremamente ampie, tanto che il par. 2 dell'art. 5 cerca di riequilibrarne la portata. Si specifica così che, nei casi consentiti, il sistema deve essere dispiegato solo a conferma dell'identità di un individuo già specificamente individuato, nel rispetto del principio di proporzionalità,<sup>43</sup> e con restrizioni temporali, geografiche e soggettive.<sup>44</sup> Le verifiche del caso debbono essere necessariamente effettuate da una *judicial authority* o una *independent administrative authority*, cui l'aspirante utilizzatore del sistema dovrà indirizzare un'apposita richiesta di autorizzazione preventiva (o successiva, in caso d'urgenza, v. art. 5, par. 3 AIA).<sup>45</sup> Le regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni dovranno però essere stabilite a livello nazionale (art. 5, par. 5 AIA).

<sup>38</sup> SACCHETTO (2020), p. 1.

<sup>39</sup> *Commission guidelines*, cit., p. 100.

<sup>40</sup> *Id.*, p. 96.

<sup>41</sup> Il criterio proposto dalla Commissione garantisce una certa flessibilità nel definire l'assenza di ritardi significativi. Ed infatti la proposta costringe a chiedersi quanto debba considerarsi esteso il «luogo di reperimento del dato biometrico». Si pensi ad esempio alla stazione Termini di Roma, la più grande d'Italia per estensione. Se la si considera un unico luogo di reperimento, allora l'identificazione ivi compiuta finirebbe per essere sempre in *real time* (quindi vietata, in via di principio), quanto meno per il tempo di permanenza dei passeggeri negli ampi locali della stazione. Ma si può ben adottare una definizione più stringente di luogo di reperimento del dato biometrico, con ciò intendendo l'area immediatamente prospiciente a quella delle telecamere: così, l'identificazione sarebbe pressoché sempre *ex post*, eccetto per quella effettuata nell'immediatezza. Forse, un criterio espresso in termini numerici (minuti, ore) avrebbe garantito maggiore certezza, pur dovendosi necessariamente scontrare con situazioni di fatto molto diverse tra loro.

<sup>42</sup> *Ibidem*.

<sup>43</sup> In particolare considerando: a) la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema; b) le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze, v. art. 5, par. 2 AIA.

<sup>44</sup> In più, potrà essere disposto solo se è stata completata la valutazione d'impatto sui diritti fondamentali e se il sistema di IA è registrato nel *database europeo* di cui all'art. 49 AIA. Tuttavia, la registrazione avviene in un'area non pubblica del *database*: v. art. 49, par. 4 AIA.

<sup>45</sup> Il secondo sottoparagrafo dell'art. 5 par. 3, rafforza il canone di proporzionalità proprio del procedimento autorizzativo, stabilendo che l'autorità incaricata della decisione debba accogliere la richiesta solo se convinta che l'utilizzo del sistema di identificazione *real time* sia necessario e proporzionato al perseguimento degli obiettivi per cui è astrattamente ammesso. In più, lo stesso sottoparagrafo stabilisce che nessuna decisione che produca un effetto sfavorevole su una persona possa essere presa solamente sulla base dei risultati prodotti dai sistemi in esame.

### 3.2.2. *Il versante interno. Il S.A.R.I. Real Time alla ricerca di una base giuridica.*

Nemmeno la polizia italiana ha resistito all'«irresistibile tentazione del riconoscimento facciale»<sup>46</sup>: il Ministero dell'Interno l'ha dotata di un applicativo denominato S.A.R.I. («Sistema Automatico di Riconoscimento delle Immagini») in grado di confrontare le immagini di *input* con una banca dati composta essenzialmente da precedenti fotosegnalamenti.<sup>47</sup>

Pur non essendo note le modalità specifiche del suo funzionamento,<sup>48</sup> si sa che il sistema, in uso ai Carabinieri e alla Polizia di Stato,<sup>49</sup> si basa su un'IA<sup>50</sup> e che è in grado di esaminare e confrontare i volti sia in modalità *real time* (sotto il nome di «S.A.R.I. Real Time»), che in modalità *ex post* («S.A.R.I. Enterprise»).

Nel primo caso, le immagini provenienti da telecamere di sorveglianza in luoghi aperti al pubblico possono essere confrontate in diretta con i volti contenuti in una *watch-list* (limitata a circa 100.000 individui) alla ricerca di una corrispondenza. Il S.A.R.I. Enterprise, invece, lavora su immagini già in possesso degli inquirenti, indipendentemente dalla data e dallo strumento di acquisizione, confrontandole con un database di grandi dimensioni (10 milioni di immagini).<sup>51</sup>

È naturalmente il modulo *Real Time* quello che più si presta alle finalità di prevenzione delle attività criminose, nonostante allo stato non si riportino effettivi casi di utilizzo del sistema da parte delle autorità italiane.

Del resto, sin dalla sua introduzione, si è discusso della sussistenza di una base giuridica idonea a sorreggerne l'utilizzo, posto che, ai sensi dell'art. 7 del d. lgs. 51/2018 (attuazione della direttiva 2016/680, c.d. «LED», *Law Enforcement Directive*), il trattamento di dati personali da parte delle autorità competenti può avvenire, di regola, solo se previsto dal diritto U.E., dalla legge, o, nei casi previsti dalla legge, da regolamento. Già nel 2021 il Garante per la protezione dei dati personali aveva rilevato l'assenza, nell'ordinamento interno, di una base giuridica idonea a legittimare un trattamento automatizzato dei dati del tipo attuato dal S.A.R.I. Real Time.<sup>52</sup>

Alla luce dell'entrata in vigore dell'AIA, e considerato che il S.A.R.I. Real Time sembrerebbe rientrare nella categoria dei sistemi di identificazione biometrica remota in *real time* in luoghi aperti al pubblico, è legittimo interrogarsi se sia sopravvenuta una legittima base giuridica fino ad oggi mancante.

La risposta pare essere negativa. Il considerando n. 38 del regolamento esplicita, infatti, che l'AIA non fornisce la base giuridica per il trattamento dei dati personali a norma della direttiva LED. Coerentemente, l'art. 5 del regolamento sembra richiedere una legge nazionale di implementazione, quasi si trattasse di una direttiva.<sup>53</sup> Ne discende che, in assenza di un intervento legislativo nazionale volto a integrare il regolamento, continua a difettare nell'ordinamento giuridico italiano una base giuridica adeguata a legittimare l'utilizzo del S.A.R.I. Real Time da parte delle autorità competenti, quale che sia la finalità perseguita.

<sup>46</sup> Sono parole del dott. Guido Scorza, ex componente del Collegio del Garante per la protezione dei dati personali, v. *Governare il futuro. L'irresistibile tentazione del riconoscimento facciale*, in *HuffPost*, 13 gennaio 2022.

<sup>47</sup> Così, ad esempio, nelle indagini per il naufragio del caicco carico di migranti *Summer Love*, avvenuto il 25 febbraio 2023 al largo di Steccato di Cutro, alcune fotografie ritraenti uno scafista sono state confrontate dal S.A.R.I. con le immagini dei fotosegnalamenti dei soggetti arrestati nel 2023 per reati afferenti all'immigrazione clandestina, fino all'identificazione di un sospettato. Cfr. *Arrestato il sesto ed ultimo scafista del naufragio di Cutro*, in *poliziadistato.it*, 7 dicembre 2023.

<sup>48</sup> Sul tema v. DELLA TORRE (2022), pp. 34-35.

<sup>49</sup> L'afferma il Viminale in [un post su X](#).

<sup>50</sup> Lo conferma il capo di Commissario Tecnico della Polizia di Stato Giovanni Tessitore in un'intervista concessa a SkyTG24, cfr. *S.A.R.I., ecco come funziona il riconoscimento facciale della polizia*, in *SkyTG24*, 13 febbraio 2020.

<sup>51</sup> Capitolato tecnico della Polizia di Stato, disponibile sul [sito della Polizia di stato](#).

<sup>52</sup> V. il Parere del Garante per la protezione dei dati personali sul S.A.R.I. Real Time, 25 marzo 2021. In risposta a tale parere nacque il d.d.l. C 3009 del 12 aprile 2021, che avrebbe dovuto portare, nelle intenzioni, alla sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico. Tale progetto divenne poi realtà con il d.l. 139/2021, il c.d. «Decreto capienze», convertito, con modificazioni dalla l. 205/2021, con cui si è stabilita la sospensione dell'installazione e utilizzazione dei sistemi di riconoscimento facciale fino al 31 dicembre 2023. Se non che, la sospensione prevede larghissime eccezioni in tema di prevenzione e repressione dei reati, come nota SACCHETTO (2022). Con l. 3 luglio 2023, n. 87 (di conversione del d.l. 10 maggio 2023, n. 51) la suddetta moratoria è stata estesa fino al 31 dicembre 2025 ma, al momento in cui il presente lavoro viene inviato all'*Editorial Advisory Board* di Questa Rivista per la pubblicazione, il termine della moratoria non risulta prorogato oltre.

<sup>53</sup> Gli stati membri «interessati» infatti, «stabiliscono» (il verbo è servile ed esprime un dovere) «le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni», ivi inclusi gli specifici obiettivi perseguibili con la ripresa *real time* (art. 5, par. 5 AIA).

Al contempo, nella stretta prospettiva processualpenalistica, le conseguenze di tale assenza appaiono contenute. Ciò in quanto l'eventuale impiego del S.A.R.I. *Real Time* pur senza una base giuridica per il trattamento dei dati non dovrebbe comportare l'inutilizzabilità del relativo *output* né altre sanzioni processuali.

Da un lato, infatti, l'uso del S.A.R.I. *Real Time* dovrebbe essere circoscritto a una fase antecedente al pervenire di una *notitia criminis*, in un momento in cui l'intervento della polizia è finalizzato alla mera tutela dell'ordine pubblico. Da un altro, anche ove successivamente la parte pubblica tentasse di utilizzare i risultati del S.A.R.I. *Real Time* in sede (cautelare o) processuale, sembrerebbero mancare «veri e propri divieti probatori»<sup>54</sup> che possano integrare fattispecie di inutilizzabilità generale ai sensi dell'art. 191 c.p.p.

Come ben noto, l'individuazione dei divieti di acquisizione determinanti inutilizzabilità è essenzialmente rimessa all'interprete.<sup>55</sup> In dottrina è pacifico che tale «sanzione» (se di sanzione si tratta) debba conseguire non solo alla violazione di divieti probatori espliciti, ma anche di divieti impliciti o indiretti, come quando la legge fa riferimento a condizioni e presupposti non rispettati nel caso concreto.<sup>56</sup> Il terreno dei divieti impliciti è incerto: per testarne la ricorrenza si suggerisce un approccio casistico, basato sulla verifica della natura dell'interesse protetto dalle disposizioni sotto esame e dell'esistenza o meno di un potere istruttorio dell'autorità giudiziaria.<sup>57</sup> Non dovrebbe, invece, comportare inutilizzabilità il mero mancato rispetto delle modalità di acquisizione della prova.<sup>58</sup> Nell'applicazione pratica di queste linee di indirizzo, tuttavia, la giurisprudenza è ondivaga: ravvisa talvolta inutilizzabilità talaltra mere irregolarità senza seguire un orientamento coerente.<sup>59</sup>

Nel caso che qui occupa, il S.A.R.I. *Real Time* manca di uno specifico apparato di condizioni e presupposti di utilizzo ritagliato *ad hoc* sul nostro ordinamento. Né, stante anche la riserva di cui al considerando n. 38 AIA, il regolamento potrebbe fungere *ex se* da base giuridica legittimante una regola di esclusione per così dire «europea».<sup>60</sup> Di conseguenza, fino all'intervento di uno statuto nazionale che regoli le garanzie alla cui violazione sia ricollegata l'inutilizzabilità, le determinazioni algoritmiche del S.A.R.I. *Real Time* saranno probabilmente ritenute utilizzabili, pur arrischiando la lesione di diritti e interessi di alta caratura.

## 4.

### L'IA come mezzo d'investigazione e di prova.

Col passaggio dalla prevenzione all'indagine, le IA assumono funzione di prova.

Il terreno probatorio è particolarmente permeabile alle innovazioni tecnologiche: queste vi si infiltrano dapprima come strumenti al servizio della polizia, ora «giudiziaria» e non più «amministrativa»<sup>61</sup>. Finiscono quindi per raggiungere il processo, ove mettono frequentemente in tensione il principio del contraddittorio nella formazione della prova.<sup>62</sup>

Già da tempo una parte della dottrina ha notato l'emersione di un dominio probatorio non sovrapponibile alla tradizionale categoria della prova digitale e più strettamente connesso, per

<sup>54</sup> *Rel. prel. al c.p.p., sub Libro III, Titolo I.*

<sup>55</sup> «Come si diagnostica l'esistenza di un divieto? Quando il divieto riguarda l'acquisizione della prova?», già si chiedeva, all'alba dell'entrata in vigore del nuovo codice, NOBILI (1990b), pp. 410-411. Per una classificazione di tipo teleologico dei divieti probatori, cfr. GALANTINI (1997), p. 690.

<sup>56</sup> V. *inter alios* NOBILI (1990b), p. 410 e CAPRIOLI (2008), p. 3528.

<sup>57</sup> CAIANIELLO (2012), p. 116. In giurisprudenza v. *ex multis* Cass. pen., sez. IV, 2 marzo 2022, n. 21304 sul 251 cpp.

<sup>58</sup> V. ad es. Cass. pen., sez. II, 15 ottobre 2019, n. 49198.

<sup>59</sup> La casistica è sterminata. Solo qualche esempio: in sede di esame dibattimentale *ex art. 210, c. VI dell'imputato di reato connesso ex art. 12, c. I, lett. c) c.p.p.* o «collegato», il mancato avvertimento di cui all'art. 64, c. III, lett. c) c.p.p. determina la inutilizzabilità della deposizione, v. Cass. pen., sez. un., 29 luglio 2015, n. 33583, *Lo Presti ed altro*. Non sono mancate tendenze giurisprudenziali volte a sanzionare con l'inutilizzabilità anche le prove acquisite, generalmente, in violazione dei diritti fondamentali della persona (v. ad es. Cass. pen., sez. III, 26 febbraio 2002, n. 7432, *Dedda ed altro* sull'individuazione fotografica operata dalla p.g. senza l'assistenza di un interprete). Al contrario, è ritenuta utilizzabile la ricognizione in dibattimento non rispettosa delle forme del 214 c.p.p. (che pure parrebbero essere condizioni e presupposti), *ex multis* Cass. pen., sez. II, 4 luglio 2013, n. 40081 e, più recentemente, Cass. pen., sez. II, 13 luglio 2022, n. 35425. Ancora, è utilizzabile l'individuazione dell'autore del furto mediante il ricorso a dati genetici contenuti in archivio informatico della p.g. non rispettoso del codice *privacy* (v. Cass. pen., sez. V, 5 dicembre 2006, n. 4430 e, più recentemente, Cass. pen., sez. II, 26 aprile 2021, n. 15577).

<sup>60</sup> È inverosimile che la Corte di Giustizia U.E., investita di una questione sul punto, imponga l'esclusione delle prove ottenute in violazione della disciplina del riconoscimento biometrico di cui all'AIA. Sul tema dell'esclusione v. in giurisprudenza Corte di Giust. U.E., cause riunite C-511/18, C-512/18 e C-520/18, 6 ottobre 2020, *La Quadrature du Net* e a.; C-746/18, 2 marzo 2021, *Prokuratuur*. In dottrina v. PANZAVOLTA e MAES (2022), pp. 208 ss.

<sup>61</sup> Sulla classica distinzione v. CAMON (2023), p. 213.

<sup>62</sup> PRESSACCO (2022), pp. 91 ss.

struttura e per logica, al paradigma dell'intelligenza artificiale.<sup>63</sup> Si tratta delle “prove generate automaticamente”<sup>64</sup>, in cui il materiale probatorio non viene semplicemente estratto da un dispositivo mediante tecniche digitali (sarebbe *digital evidence*), ma è generato, in quanto tale, da un processo computazionale.<sup>65</sup> In altri termini, è l'algoritmo a trasformare un *input* in un *output* dotato di rilevanza probatoria. Si pensi, ad esempio, ai *software* progettati per l'elaborazione di profili genetici complessi, utilizzati nell'analisi del DNA in ambito forense (v. *infra*).

Il presente paragrafo distingue tra cinque famiglie di IA *lato sensu* “probatorie”:

- Sistemi biometrici impiegati per l'identificazione da remoto (ma non in *real time*: quell'impiego è tipico della fase preventiva);
- Sistemi biometrici impiegati per l'identificazione, ma non da remoto;
- Sistemi biometrici impiegati per scopi diversi dall'identificazione;
- Sistemi non biometrici a uso investigativo e probatorio;
- Sistemi per il calcolo del rischio di recidiva (*risk assessment tools*)

## 4.1. *Sistemi biometrici per l'identificazione da remoto, ma non in real time.*

### 4.1.1. *Generalità. La regolamentazione europea dell'identificazione remota differita.*

Come anticipato, i sistemi di identificazione biometrica remota non trovano impiego esclusivamente in chiave preventiva, ma possono essere utilizzati anche con finalità propriamente investigative e probatorie. Anche in questo caso, è il volto il carattere più sfruttato per l'identificazione: nell'esperienza italiana si registra una prassi consolidata di utilizzo del S.A.R.I. *Enterprise*, la versione *ex post* del *software* di riconoscimento facciale in uso alle nostre forze dell'ordine.<sup>66</sup>

Anche per queste IA il regolamento prescrive un'autorizzazione rilasciata da un'autorità giudiziaria o amministrativa (art. 26, par. 10 AIA). Manca però l'attributo «indipendente», quindi l'autorizzazione potrà ben essere concessa da un'autorità posta sotto il controllo del Governo.<sup>67</sup> L'autorizzazione, peraltro, non deve nemmeno necessariamente precedere l'attivazione del sistema: il regolamento consente che venga rilasciata «senza indebito ritardo» entro 48 ore, senza subordinare tale possibilità alla sussistenza di una situazione d'urgenza (v. ancora art. 26 AIA).

V'è di più. L'autorizzazione non va richiesta se il sistema serve all'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato.<sup>68</sup> È il caso più frequente: i sistemi *ex post* vengono solitamente impiegati immettendovi i dati di *input* (come un'immagine di una telecamera a circuito chiuso) appositamente per una «identificazione iniziale». Dati, peraltro, certamente riferibili a «fatti oggettivi e verificabili direttamente connessi al reato» (ad esempio, una rapina). Al di là dei proclami, il riconoscimento biometrico *ex post* rimarrà dunque una attività pienamente nelle mani della polizia giudiziaria.

Seppure queste garanzie procedurali appaiano blande, sul lato tecnico l'AIA impone ai

<sup>63</sup> QUATTROCOLO (2023), pp. 477 ss.

<sup>64</sup> PALMIOTTO (2023), p. 24; QUATTROCOLO (2020), p. 74.

<sup>65</sup> V. in generale GLESS (2020).

<sup>66</sup> Tuttavia, anche i sistemi *real time* possono essere utilizzati fuori dal contesto preventivo, come risulta evidente dall'elenco di eccezioni al divieto di cui all'art. 5, par. 1, lett. h) AIA, il quale menziona anche attività propriamente investigative. L'associazione tra IA per uso probatorio e sistemi *ex post* è arbitraria, ma ben si adatta alla realtà italiana.

<sup>67</sup> La Corte di Giustizia dell'Unione europea ha sviluppato una copiosa giurisprudenza sul tema dell'indipendenza delle autorità giudiziarie in materia di cooperazione internazionale penale. A titolo di esempio, la Corte ha negato che la Procura austriaca, posta sotto il controllo del Ministero della Giustizia austriaco, goda dell'indipendenza necessaria a emanare un mandato d'arresto europeo senza la convalida di un tribunale (caso C-489/19, 9 ottobre 2019, *PPU NJ (Parquet de Vienne)*). Mancando, all'art. 26, par. 10 AIA, l'aggettivo «indipendente», non dovrebbero esservi ostacoli nel consentire a un ufficio di Procura posto sotto il controllo del Governo di autorizzare l'identificazione biometrica. Specularmente, se si tratterà di un'autorità amministrativa, non varranno i requisiti di indipendenza imposti dalla medesima Corte nel caso C-470/21, 30 aprile 2024, *La Quadrature du Net and Others v Premier ministre and Ministère de la Culture*, par. 126, per cui «in ambito penale, il requisito dell'indipendenza implica che l'autorità responsabile di tale controllo previo, da un lato, non sia coinvolta nella conduzione dell'indagine penale in questione e, dall'altro, abbia una posizione di neutralità rispetto alle parti del procedimento penale».

<sup>68</sup> Nei pochi casi in cui l'autorizzazione rimarrà atto dovuto, il diniego della stessa comporterà l'interruzione dell'uso del sistema di identificazione e la cancellazione dei relativi dati personali (v. ancora art. 26, par. 10 AIA).

sistemi di riconoscimento *ex post* il rispetto di pervasivi obblighi di *compliance*.

Vi sono, in primo luogo, le prescrizioni dettate in materia di qualità e *governance* dei dati per i sistemi classificati ad alto rischio (art. 10 AIA). La disposizione introduce principi in tema di pertinenza, rappresentatività e correttezza dei dati impiegati (art. 10, par. 2 e 3 AIA), prevedendo altresì meccanismi di controllo volti a prevenire il manifestarsi di distorsioni discriminatorie nell'*output* del sistema.

L'AIA costringe poi i *deployer* di sistemi ad alto rischio a dotarsi di una documentazione tecnica (art. 11 e all. IV AIA) che investa tanto la struttura del sistema quanto il suo processo evolutivo: dall'architettura alle modalità di addestramento, dalle misure di supervisione umana al *testing*. A ciò si affiancano prescrizioni in tema di accuratezza, robustezza e cybersicurezza (art. 15 AIA), da garantire secondo parametri elaborati dalla Commissione con altri *stakeholders* (art. 15, par. 1 e 2 AIA). Le metriche prestazionali dovrebbero, in linea generale, confluire nelle istruzioni d'uso, anche se queste, in linea di principio, non saranno ostensibili alla difesa.<sup>69</sup>

Per l'identificazione biometrica a distanza, l'AIA prevede poi obblighi di documentazione più stringenti rispetto a quelli stabiliti per gli altri sistemi ad alto rischio. In particolare, l'art. 12, par. 3 introduce un regime di *record-keeping* rafforzato, imponendo che il sistema conservi, in maniera automatizzata, informazioni sull'intera sequenza operativa: dalle tempistiche dell'attività (momento iniziale e finale) al *database* utilizzato per la comparazione, fino ai dati di *input* e l'identità delle persone coinvolte nel controllo del risultato fornito dall'algoritmo. Se resi accessibili anche solo parzialmente alla difesa, eventualmente su ordine del giudice, tali dati potrebbero consentire una forma di scrutinio *ex post* dell'attività algoritmica e un controllo (indiretto) sull'affidabilità dell'identificazione.

Ancora, il regolamento impone, in materia di identificazione biometrica, una supervisione umana (*human oversight*) rinforzata, che deve coinvolgere almeno due persone dotate delle competenze necessarie a compiere tale controllo (art. 14, paragrafo 5 AIA).<sup>70</sup>

Infine, l'art. 26, par. 10, AIA stabilisce che l'utilizzo dei sistemi di identificazione biometrica *ex post* debba essere debitamente documentato nel «fascicolo di polizia» e reso disponibile alle autorità competenti per la vigilanza sul mercato e per la protezione dei dati personali. La disposizione, tuttavia, non sembra richiedere che tale documentazione venga inserita in un fascicolo accessibile alla persona sottoposta al procedimento. Piuttosto, essa ne impone la trasmissione esclusivamente alle autorità di controllo amministrativo. Si tratta, con ogni evidenza, di una scelta normativa poco ambiziosa, che avrebbe potuto – e forse dovuto – essere corretta imponendo, in via generale, la disponibilità dei dati alla difesa, quale garanzia minima di trasparenza e possibilità di controllo difensivo.

La disciplina appena descritta non si applicherà solamente ai sistemi di riconoscimento facciale *ex post*, cui pure evidentemente il legislatore europeo intendeva riferirsi nel regolamentare i sistemi di identificazione remota. Saranno sottoposte al medesimo regime tutte le IA coinvolte nell'identificazione attraverso caratteri che non richiedano il «coinvolgimento attivo» dell'identificando (art. 3, par. I, n. 41) AIA).

## 4.1.2. *I risvolti sull'impiego del S.A.R.I. Enterprise durante le indagini e sull'utilizzabilità processuale dei risultati.*

In considerazione del loro concreto impiego nel contesto italiano, ci si concentrerà ora sugli effetti che il regolamento produrrà sui sistemi di riconoscimento biometrico *ex post* basati sul volto, con particolare attenzione al S.A.R.I. *Enterprise*. Resta inteso che analoghe considerazioni potrebbero valere anche per le IA che comparano, da remoto, caratteristiche biometriche diverse (v. anche *infra*, par. 4.2).

Operativo dal 2018, il S.A.R.I. *Enterprise* è stato introdotto senza che, in fase preliminare, il Garante per la protezione dei dati personali sollevasse rilievi critici in ordine alla compatibilità con la disciplina sulla protezione dei dati.<sup>71</sup> A consentirne l'impiego vi sarebbero infatti

<sup>69</sup> Le IA ad alto rischio impiegate nelle attività di contrasto rimangono esonerate dall'obbligo di includere tali informazioni nella banca dati europea, generando un evidente *vulnus* informativo (all. VIII, sez. A, n. 12 AIA).

<sup>70</sup> Realisticamente, si tratterà di ufficiali o agenti di polizia giudiziaria. Ma l'obbligo non è assoluto: ove il diritto europeo o la legge nazionale lo ritenesse sproporzionato, è ammesso derogarvi, tra gli altri, nel campo del *law enforcement* (art. 14, par. 5 AIA).

<sup>71</sup> Cfr. le Osservazioni del Garante per la protezione dei dati personali sul sistema automatico di ricerca dell'identità di un volto S.A.R.I.

plurime basi giuridiche, tra cui l'art. 4 del t.u.l.p.s. (r.d. 18 giugno 1931, n. 773) e l'art. 349 c.p.p. in materia di identificazione di persone a opera della polizia giudiziaria. Tanto basterebbe, per il Garante, a rispettare l'art. 7 del d.lgs. n. 51/2018 (attuazione della direttiva "LED") in materia di trattamento di categorie particolari di dati personali da parte delle autorità. Tuttavia, la questione è più complessa.<sup>72</sup>

È vero che l'indagine a mezzo del S.A.R.I. è sussumibile sotto il cappello dell'art. 349 c.p.p. quando viene dispiegato per l'identificazione dell'indagato.<sup>73</sup> Fuori da questi casi, però, il S.A.R.I. *Enterprise* sembrerebbe piuttosto assumere i tratti di un'indagine atipica, non dissimile, nella sostanza, dal riconoscimento fotografico svolto dalla polizia giudiziaria.<sup>74</sup> Si collocerebbe così al di fuori di un qualsiasi perimetro normativo definito, senza una disciplina che stabilisca, in modo espresso, presupposti, limiti e modalità di utilizzo del sistema.

Per un altro verso, fonti di polizia hanno suggerito di ricondurre l'uso del S.A.R.I. *Enterprise* nell'alveo delle attività di accertamento tecnico ex art. 359 c.p.p., anche al fine di garantirne l'utilizzabilità dibattimentale.<sup>75</sup> Nemmeno questa opzione ha soddisfatto la dottrina: il *software* S.A.R.I. mancherebbe totalmente dei crismi di scientificità propri degli accertamenti tecnici. Emerge, in modo particolare, la mancanza di trasparenza circa gli indicatori di sicurezza e affidabilità del sistema, a cominciare dal tasso di falsi positivi.<sup>76</sup>

Anche in merito all'utilizzabilità processuale dei risultati offerti dal S.A.R.I. *Enterprise* gli studiosi hanno espresso sentite riserve. Si tratterebbe, secondo l'opinione dominante, di una ricognizione atipica, sempre in ragione del fatto che il ricognitore è una macchina e non un umano, come richiesto propriamente dall'art. 213 c.p.p. L'atipicità dovrebbe attivare, per quel che valgono,<sup>77</sup> le salvaguardie del 189 c.p.p.: senonché, secondo la medesima dottrina, mancherebbero al S.A.R.I. *Enterprise* tanto l'idoneità all'accertamento dei fatti (perché non è dato sapere il funzionamento dell'algoritmo "ricognitore") quanto l'attitudine a rispettare la libertà morale degli individui, per via delle modalità di impiego dei loro dati personali.<sup>78</sup>

Il diritto pretorio semplifica: l'analisi della giurisprudenza di merito mostra una prassi ben consolidata in favore dell'utilizzabilità dei risultati del S.A.R.I. L'operante di polizia giudiziaria, escusso in sede dibattimentale per riferire sulle attività compiute nel corso delle indagini, riferisce di aver fatto ricorso al S.A.R.I., il quale gli ha restituito una lista di individui ordinata secondo una scala decrescente di probabilità di *match*. In cima v'è l'imputato di turno, già presente negli archivi informatici della polizia perché in precedenza fotosegnalato.<sup>79</sup> Così come il riconoscimento fotografico operato dalla polizia giudiziaria, anche il suo "gemello digitale", nato con finalità endoprocedimentali, entra dunque nel processo attraverso la testimonianza, "esperta" o meno, del *deployer* (la polizia). L'identificazione algoritmica non viene mai reiterata dinanzi al giudice del dibattimento, nonostante nulla, in linea di principio, lo impedisca, trattandosi di operazione tecnicamente replicabile all'infinito.<sup>80</sup>

Quanto poi alla valutazione, nemmeno risultati pessimi dell'algoritmo ricognitore arrestano la «bulimia istruttoria»;<sup>81</sup> in un caso, un coefficiente probabilistico del riconoscimento del 60,42% è stato ritenuto sufficiente a rendere l'identificazione dell'imputato «assolutamente

*Enterprise*, 26 luglio 2018. Per una ricostruzione: LOPEZ (2019), pp. 248 ss.

<sup>72</sup> Tra le voci critiche dell'opinione del Garante v., per tutti, GIALUZ (2021), pp. 51 ss.

<sup>73</sup> L'art. 349 c.p.p. ha un dettato letterale molto ampio: permette infatti alla polizia giudiziaria di svolgere «altri accertamenti» ai fini dell'identificazione, cfr. DELLA TORRE (2022), p. 36, nota 129 e i riferimenti ivi citati.

<sup>74</sup> LOPEZ (2019), p. 253.

<sup>75</sup> Lo riporta DELLA TORRE (2022), p. 40 citando [una fonte ministeriale](#), secondo cui «sono però sempre gli operatori specializzati della Polizia scientifica ad effettuare la necessaria comparazione fisionomica». Questo, in caso di "match", consente di integrare l'utilità investigativa del risultato anche con un accertamento tecnico a "valenza dibattimentale", 7 settembre 2018.

<sup>76</sup> MARANDOLA (2023), p. 512.

<sup>77</sup> Epitome del rifiuto del principio di tassatività (cfr. in dettaglio NOBILI (1990a), p. 398), l'art. 189 c.p.p. è da sempre al centro del dibattito tra chi ritiene che esso richieda un "titolo logico" superiore all'art. 190 c.p.p. per l'ammissione delle prove, cfr. tra gli altri CANZIO (2022), p. 903; DOMINIONI (2005), p. 212. LORUSSO (2009), p. 31 nota che anche ove effettivamente vi sia una differenza tra 189 e 190 c.p.p. quanto a titolo logico, comunque la fase di ammissione non permetterebbe di renderla evidente se non in casi estremi.

<sup>78</sup> GIALUZ (2025), p. 13; DELLA TORRE (2020), p. 242.

<sup>79</sup> V. ad es. Trib. Ascoli Piceno, sez. pen., 20 luglio 2022, n. 452 in *OneLegale*, p. 2; Trib. Nola, sez. pen., 11 gennaio 2024, n. 2055, p. 3, *ibidem*, apparentemente con il coinvolgimento della Polizia Scientifica; nel caso deciso da C. App. Roma, sez. II pen., 2 ottobre 2023, n. 10003 in *OneLegale* (con rito abbreviato) invece, il S.A.R.I. è stato utilizzato per la creazione di un "fascicolo fotografico" contenente 6 immagini da sottoporre alla persona offesa per l'identificazione fotografica.

<sup>80</sup> LOPEZ (2019), p. 257, secondo cui «unico oggetto di confronto dialettico con l'accusa riguarderà soltanto la fonte mediata, ossia la relazione della polizia scientifica illustrativa della verifica di affidabilità dell'output, attraverso gli standard identificativi classici, fondati su parametri discriminatori sia metrici (ad esempio, distanza degli occhi, altezza degli zigomi, posizione reciproca tra naso e bocca, ecc.), che fisionomici».

<sup>81</sup> L'espressione è di CORDERO (2012), p. 24.

certa» in quanto confermata dall'operatore umano.<sup>82</sup> Addirittura alla Cassazione basta il 54%, ove a determinare la *défaillance* del sistema abbia concorso il presunto rapinatore, che alla telecamera ha rivolto, divertito, una «smorfia con la bocca»<sup>83</sup>. Neanche a dirlo, queste percentuali così basse sono ammesse a patto che a utilizzare il S.A.R.I. sia la parte inquirente: quando è l'imputato a chiedere un «disconoscimento», il *software* diviene inaffidabile e privo di validazione scientifica.<sup>84</sup>

Questo, in sintesi, il quadro giuridico nazionale in cui si innesta il regolamento: un contesto strutturalmente divaricato tra le ambiziose istanze garantistiche coltivate in sede dottrinale e il loro sistematico rifrangersi, talvolta sino al collasso, sul piano della prassi applicativa.

Orbene, pur rimanendo impregiudicata la necessità di una apposita legge attuativa a regolare l'utilizzo del S.A.R.I.,<sup>85</sup> il nuovo quadro normativo europeo produrrà, di per sé, importanti externalità positive sulla sua procedimentalizzazione.

Durante le indagini, l'innalzamento degli *standard* tecnici dovrebbe imporre la sussunzione del S.A.R.I. nell'alveo dell'art. 359 c.p.p. (accertamenti tecnici ripetibili). Per l'effetto, a dibattimento, l'*output* algoritmico dovrebbe poter aspirare a valenza probatoria solo a seguito dell'esame del consulente, dell'acquisizione della relazione tecnica, nonché della ripetizione delle operazioni di confronto in un contesto dialettico e garantito.<sup>86</sup>

In ambito cautelare, ove mancano sia la possibilità di escutere un consulente esperto sia quella di ripetere le operazioni tecniche,<sup>87</sup> l'impiego dei sistemi di identificazione andrebbe compensato da un'elevata soglia di attendibilità del dato scientifico, con percentuali di compatibilità prossime alla certezza. Ad imporre una tale cautela, al di là del buon senso, sta il dato formale per cui solo indizi «gravi» possono giustificare la restrizione provvisoria della libertà (art. 273 c.p.p.). Come noto, la definizione dello *standard* di prova richiesto in sede cautelare, specie quando vengano in considerazione prove critiche come l'identificazione di un'IA, è oggetto di un annoso dibattito in dottrina e giurisprudenza.<sup>88</sup> Sta di fatto che, ad oggi, il riconoscimento fotografico (umano) viene considerato sufficiente a fondare il titolo cautelare «in assenza di profili di inattendibilità»<sup>89</sup>. Se così è, anche alle identificazioni operate dall'IA dovrebbe essere affidato quantomeno un valore indiziario, ove sia alto il coefficiente di probabilità di *match* tra la persona sottoposta alle indagini e l'identificando.<sup>90</sup>

In termini più generali, questa e altre indagini compiute a mezzo di IA andrebbero procedimentalizzate nell'ottica della parità di trattamento con gli altri mezzi di prova: la pur giusta attenzione che si rivolge ai possibili *biases* algoritmici non dovrebbe oscurare quelli propri delle valutazioni umane, le quali cadono facilmente vittime di argomenti suggestivi e sovente si affidano a criteri decisionali vaghi.<sup>91</sup> Si pensi ad esempio all'individuazione di persone, mezzo di prova del quale è nota la scarsa attendibilità, dovuta essenzialmente a ragioni neuropsico-

<sup>82</sup> Tribunale di Trieste, n. 820 del 19 agosto 2024, in *OneLegale*, p. 3: «Assolutamente certa è l'identificazione degli autori del fatto negli odierni imputati: il confronto tra le fotografie dei rispettivi cartellini identificativi e le immagini dei volti nitidamente immortalati dalla telecamera di videosorveglianza non lasciano davvero alcun margine di dubbio, confermando il risultato di *screening* compiuto tramite il sistema di riconoscimento automatico "S.A.R.I.", che già aveva offerto un risultato dotato di elevata attendibilità, in ragione dell'alta percentuale attestata e corroborata dall'assenza di corrispondenze degni di rilievo con altri soggetti».

<sup>83</sup> Cass. pen., sez. II, 22 gennaio 2025, n. 2613, *Perfetti*.

<sup>84</sup> Cass. pen., sez. IV, 18 giugno 2019, n. 39731. Sulle potenzialità d'uso dell'IA da parte della difesa, v. LASAGNI (2022), pp. 63 ss.

<sup>85</sup> La l. 23 settembre 2025, n. 132 prevede una delega al Governo affinché provveda a emanare una «apposita disciplina per l'utilizzo di sistemi di intelligenza artificiale per l'attività di polizia» (art. 24, c. II, lett. b) l. cit.). Nell'esercizio della delega, il Governo dovrà regolamentare l'utilizzo delle IA nelle indagini preliminari «nel rispetto delle garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza» (art. 24, c. V, lett. e) l. cit.).

<sup>86</sup> È pacifico che l'esame di consulenti e periti debba avvenire nel pieno rispetto del contraddittorio «in tutte le fasi che caratterizzano la formazione della prova», cfr. Cass. pen., sez. 1, 17 febbraio 2023, n. 39832. L'equiparazione vale anche per il caso della rinnovazione in appello della prova decisiva, come notoriamente affermato dalla Cass. pen., sez. un., 28 gennaio 2019, n. 14426, *Pavan*.

<sup>87</sup> Per un'opinione favorevole alla possibilità di esercitare il diritto al contraddittorio nella formazione della prova anche in fase cautelare, v. MOLARI (2002), pp. 137 ss.

<sup>88</sup> La questione riguarda in particolare se nella valutazione degli «indizi» citati dall'art. 273 c.p.p. si debbano rispettare i requisiti imposti, in via generale, dall'art. 192 comma II, c.p.p., oppure no. Per un'attenta disamina degli orientamenti sul tema v. PASSALACQUA (2020).

<sup>89</sup> «Perché lascia fondatamente ritenere che sbocchi in un atto di riconoscimento, formale o informale, o in una testimonianza che tale riconoscimento confermi», così Cass. pen., sez. II, 13 maggio 2025, n. 23917, richiamando il noto precedente di Sez. II, 15 gennaio 2004 n. 5043, *Acanfora*. In un altro caso si è richiesta l'«assoluta certezza», se il riconoscimento è avvenuto a «distanza di tempo considerevole dalla commissione del fatto» (Cass. pen., sez. II, 17 settembre 2025, n. 31242).

<sup>90</sup> Meno netto è invece il limite con riguardo alle perquisizioni, considerando che eventuali operazioni della polizia giudiziaria condotte in spregio del canone dei «fondati motivi» (e quindi sulla base di un riconoscimento algoritmico inattendibile) difficilmente porterebbero alla declaratoria di inutilizzabilità del verbale di perquisizione. Ampiamente sul tema DINACCI (2023).

<sup>91</sup> CONTISSA ET AL. (2019), pp. 630 ss. osservano che in ciò si riconoscerebbe una somiglianza tra gli umani e le *black boxes* digitali.

logiche.<sup>92</sup> Sarebbe del tutto irragionevole continuare a consentire l'individuazione operata dagli umani, del tutto slegata da qualsivoglia standard di scientificità, e al contempo impedire il riconoscimento biometrico tramite *software*. In ciò, l'IA mette a nudo l'imprecisione epistemologica di prove analogiche a cui siamo forse più avvezzi, ma che non per questo dovrebbero essere considerate più attendibili.<sup>93</sup>

## 4.2.

### *Sistemi biometrici impiegati per l'identificazione, ma non da remoto.*

Sebbene la potenziale pervasività delle IA per l'identificazione remota abbia attratto su tali sistemi la maggior parte delle attenzioni dei negoziatori del regolamento, non tutte queste tecnologie biometriche operano a distanza.

Il confine tra IA "da remoto" e non si trae dalla parte definitoria del regolamento (v. art. 3, par. I, n. 41) AIA) e si fonda sulla ricorrenza di un «coinvolgimento attivo» dell'identificando. Rimane tuttavia incerto quale livello di coinvolgimento si richieda per esentare un sistema dallo statuto dell'identificazione biometrica a distanza.<sup>94</sup>

La distinzione è particolarmente importante per le IA che utilizzano, per l'identificazione biometrica, l'analisi di caratteri quali il DNA o le impronte digitali. Ad esempio, nelle indagini genetiche si riscontra un sempre maggiore impiego di *software* di genotipizzazione probabilistica, che attraverso calcoli statistici tentano di oggettivizzare l'interpretazione di profili genetici "misti", ovvero caratterizzati dalla presenza di più contributori.<sup>95</sup> L'uso di IA è riportato anche nella comparazione delle impronte digitali: il *software* setaccia le banche dati in pochi secondi alla ricerca di un *match*, velocizzando processi altrimenti dispendiosi in termini di tempo e risorse.<sup>96</sup> La dinamica è analoga a quella del riconoscimento facciale, ma le modalità di reperimento del dato di *input* no: l'impronta digitale può ottenersi sia attraverso il «coinvolgimento attivo» di una persona, ovvero attraverso le classiche le procedure di identificazione (c.d. fotosegnalamento); sia attraverso l'analisi delle c.d. "tracce latenti".<sup>97</sup>

Sicché IA come queste sembrerebbero essere sottoposte a una disciplina differente a seconda delle modalità di reperimento del dato biometrico, con il coinvolgimento attivo della persona da identificare oppure no. Nel primo caso l'IA andrebbe sottoposta semplicemente alla regolamentazione prevista per i sistemi ad alto rischio, trattando essa dati biometrici a fini identificativi ai sensi dell'allegato III, n. 6, lett. e) AIA. Al contrario, ove il dato di *input* sia reperito senza il coinvolgimento attivo della persona da identificare, varranno in larga misura le considerazioni già riportate in tema di sistemi biometrici per l'identificazione remota, e quindi anche le specifiche garanzie previste in questi casi.<sup>98</sup>

## 4.3.

### *Sistemi biometrici impiegati per scopi diversi dall'identificazione.*

Abbondano nell'AIA disposizioni specifiche sui sistemi che trattano dati biometrici per scopi diversi dall'identificazione. Si tratta essenzialmente di tre categorie di *software*:

- i poligrafi e gli strumenti ad essi analoghi (all. III, n. 6);
- i sistemi di riconoscimento delle emozioni (all. I, n. 1, lett. c)<sup>99</sup>, finalizzati a riconoscere o inferire «emozioni di persone fisiche sulla base dei loro dati biometrici» (art. 3, n.

<sup>92</sup> SACCHETTO (2020), pp. 4 ss.

<sup>93</sup> CAIANIELLO (2021), pp. 1 ss., in tema di *preventive justice*.

<sup>94</sup> L'intervento consapevole delle persone per fornire i dati di input da comparare, comunque, dovrebbe certamente esentare da quelle prescrizioni. V., per talune esemplificazioni, le *Commission guidelines*, cit., sub parr. (304) ss.

<sup>95</sup> Il riferimento è al *software* americano *TrueAllele*, che utilizza dichiaratamente IA: «Using artificial intelligence and applied mathematics, the company delivers vital forensic DNA identification to the criminal justice system» in [www.cybgcn.com/](http://www.cybgcn.com/). Per una prospettiva su questi sistemi v. GARRETT E RUDIN (2024). Sulla genotipizzazione probabilistica v. PICCININI E GENNARI (2021), p. 38.

<sup>96</sup> Cfr. *AI and policing: the benefits and challenges of artificial intelligence for law enforcement* del 23 settembre 2024, cit., p. 26.

<sup>97</sup> Sull'uso probatorio delle impronte digitali v. GENNARI (2016), pp. 19 ss. Per una recente applicazione dell'IA all'analisi delle impronte digitali latenti v. RAJS ET AL. (2025).

<sup>98</sup> In alcuni Stati degli Stati Uniti, i risultati prodotti dai *software* per l'analisi automatizzata delle tracce miste (come *TrueAllele*) vengono comunemente sottoposti al c.d. test di *Daubert*, v. Ct. of *Common Pleas Cuyahoga county, Ohio v. Carter*, Case No: CR-21-66065 7-A, 30 maggio 2024.

<sup>99</sup> L'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di questi sistemi è infatti proibito solo nel luogo di lavoro e negli istituti di istruzione (art. 5, par. 1, lett. f) AIA).

39 AIA); e

- i sistemi di categorizzazione biometrica (all. III, n. 1), lett. a) AIA), usati per direzionare un determinato dato a questa o a quella categoria predeterminata.

Si considerino innanzitutto le prime due applicazioni, che sono accomunate dal medesimo fine, quello di carpire dal dichiarante informazioni diverse da quelle che egli intende coscientemente riferire all'interrogante. Nonostante la loro intrusività nell'intima sfera della personalità umana il regolamento non li vieta, ma li colloca nella categoria "ad alto rischio".

Pur se ammesso a livello sovranazionale, sul fronte interno il poligrafo è ricondotto comunemente al divieto di cui all'art. 188 c.p.p. (libertà morale della persona nell'assunzione della prova), anche laddove il dichiarante vi si sottoponesse volontariamente. Sarebbe inammissibile, infatti, trarre un convincimento dal mutamento dei parametri fisiologici di un soggetto, che resterebbe in balia di strumenti dotati di scarsissima attendibilità.<sup>100</sup>

Rispetto ai sistemi di riconoscimento delle emozioni potrebbe, invece, avere senso un atteggiamento più possibilista: essi non richiedono alcun contatto attivo con l'esaminando, né sembrerebbero in grado di causare coercizioni morali più intense di quelle cagionate dalla *cross-examination* o da un interrogatorio. Sicché, nel nostro ordinamento la linea del processualmente lecito dovrà ricavarsi sulla falsariga della disciplina – di diretta derivazione costituzionale – in materia di diritto al silenzio.<sup>101</sup> Certo, anche in questo caso dovrebbero essere soddisfatti i requisiti, già imposti dalla nostra Cassazione nel campo dell'accertamento scientifico del nesso di causa – nella nota sentenza n. 43786/2010, *Cozzini* – e già richiamati, peraltro, in tema di *behavioural screening*, una forma di analisi della coerenza tra il contenuto delle espressioni verbali utilizzate nel corso di una deposizione e il linguaggio del corpo.<sup>102</sup>

Anche la classe dei sistemi di categorizzazione biometrica, pur maneggiando dati biometrici, non se ne serve per fini d'identificazione. Ed invero questi sistemi sono programmati per inserire semplicemente i dati di *input* all'interno di una determinata categoria di *items*. Ad esempio, una serie di immagini rinvenuta nell'*hard disk* dell'imputato può essere classificata a seconda dell'età, del sesso o dell'etnia del soggetto che vi è ritratto.<sup>103</sup> Il contributo di questi sistemi all'efficienza investigativa è sensibile (soprattutto per *datasets* di grandi dimensioni), giacché permettono di non delegare a un agente di p.g. la visione e la classificazione delle immagini, con evidente risparmio di risorse.

I sistemi di categorizzazione biometrica sono formalmente vietati dall'art. 5, par. 1, lett. g) AIA se usati per dedurre l'appartenenza di un soggetto a determinati gruppi sensibili.<sup>104</sup> Tuttavia, vige un'ampia eccezione per le attività compiute dall'autorità di contrasto, se i dati sono acquisiti legalmente. I sistemi ammessi dovrebbero comunque essere ritenuti ad alto rischio (all. III, n. 1), lett. a) AIA).

Come per i *software* che identificano, anche per quelli che semplicemente classificano si pone un tema (sostanzialmente non risolto dall'AIA) di parità delle armi. Ad esempio, la difesa potrebbe nutrire un interesse a replicare l'operazione di categorizzazione al fine di dimostrare che la presenza di immagini illecite è statisticamente irrilevante, e dunque frutto di uno scaricamento casuale o automatico.<sup>105</sup> Per evitare di compromettere l'equilibrio dialettico del processo, si potrebbe allora pensare ad un *software open source*, che sia contemporaneamente in grado di rispettare gli *standard* richiesti dal regolamento e liberamente disponibile anche alle parti che subiscono il trattamento. Oppure ancora, autorevole dottrina aveva proposto di istituire un albo di *software* proprietari ma validati *ex ante*, al quale l'imputato possa ricorrere per ottenere una seconda verifica sul risultato algoritmico (*redundancy approach*).<sup>106</sup> Si tratta evidentemente di soluzioni che, nel silenzio del legislatore europeo, dovranno essere vagliate

<sup>100</sup> Sul tema v. tra gli altri, CORDERO (1992), p. 229; DOMINIONI (2005), p. 214; GRIFANTINI (2005), p. 530; LUPARIA (2006), pp. 101 ss. Ed invero l'intento del legislatore del 1988 era propriamente quello di impedire l'uso di mezzi di «subdola persuasione»: «l'accento cade soprattutto su narcoanalisi, *lie detector*, ipnosi e siero della verità che si ritiene debbano essere banditi dalla sede processuale anche per la scarsa attendibilità che viene loro generalmente riconosciuta» (*Rel. prel. al c.p.p., sub libro III, titolo I*).

<sup>101</sup> V., in generale, CAMON (2023), p. 150.

<sup>102</sup> Cass. pen., sez. I, 18 giugno 2020, n. 27115. Sul *Facial Action Coding System*, un metodo di analisi del comportamento non verbale che analizza, in particolare, le contrazioni muscolari del volto v. JELOVICICH (2014).

<sup>103</sup> *AI and policing: The benefits and Challenges of Artificial Intelligence for Law Enforcement*, cit., pp. 13 ss.

<sup>104</sup> In particolare: razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale. Si noti che manca un dato fondamentale: l'età.

<sup>105</sup> Il riferimento è alla nota vicenda del materiale rinvenuto nel computer di Alberto Stasi nell'ambito delle indagini sul c.d. delitto di Garlasco, per cui v. Cass. pen., sez. III, 5 marzo 2014, *Stasi*.

<sup>106</sup> CONTISSA ET AL. (2019), p. 634.

dai singoli Stati membri.

## 4.4.

### *Sistemi non biometrici a uso investigativo e probatorio.*

V'è poi una grande categoria residuale che comprende molte IA non biometriche dalle funzionalità più varie, come quelle in grado di elaborare modelli 3D della scena del crimine<sup>107</sup> o di ricostruire eventi balistici.<sup>108</sup>

L'AIA non dedica molta attenzione a questi sistemi *lato sensu* probatori.<sup>109</sup> L'unica indicazione proviene dalla classificazione come ad alto rischio dei sistemi destinati a essere utilizzati dalle autorità di contrasto (o per loro conto) per «valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati» (all. III (1), n. 6, lett. c) AIA).

Da un punto di vista soggettivo, quindi, il consulente della difesa sarebbe escluso: non è autorità di contrasto né agisce per suo conto. Da quello oggettivo, invece, bisogna intendersi sul significato dell'espressione «elementi probatori». Data la natura sovranazionale della fonte normativa in esame, non è plausibile che si tratti di un riferimento al significato tecnico di informazione non ancora oggetto di valutazione del giudice.<sup>110</sup> La disposizione dovrà essere quindi intesa in senso atecnico e più generale: vi rientrerebbe, ad esempio, un *software* che calcoli i possibili percorsi del proiettile sparato da un determinato punto dello spazio, nonostante esso non operi alcuna valutazione di attendibilità di un elemento probatorio ma ne produca uno *ex novo*.

La qualificazione di tali sistemi come ad alto rischio comporta ricadute giuridiche di rilievo, tra cui l'applicazione delle prescrizioni dell'AIA in materia di trasparenza, sicurezza e qualità descritti in precedenza. In questo ambito, assumerà importanza cruciale la garanzia di elevati *standard* nella costruzione del *training dataset*, nella progettazione del sistema e nella sua intellegibilità, seppure le informazioni soggette a registrazione siano estremamente limitate in caso di sistemi impiegati nei settori delle attività di contrasto (allegato VIII, sez. A, n. 12 AIA).

Le verifiche sul rispetto della disciplina tecnica saranno poi rimesse alla sede dibattimentale, ove periti e consulenti tecnici faranno verosimilmente da «interpreti digitali» tra le domande delle parti e la macchina, come peraltro già si osserva negli Stati Uniti.<sup>111</sup> Agli esperti, dunque, spetteranno le risposte in merito alla «raccolta dei dati archiviati, la loro classificazione e le loro connessioni».<sup>112</sup>

## 4.5.

### *Sistemi per il calcolo del rischio di recidiva (risk assessment tools).*

### 4.5.1.

#### *La valutazione automatica dei precedenti dell'imputato: generalità.*

Gli strumenti di valutazione del rischio di delinquenza (più noti come *risk assessment tools*) predicono la probabilità che un soggetto cada o ricada nel crimine<sup>113</sup> o, comunque, si sottragga al processo,<sup>114</sup> basandosi sulla valutazione di fattori di rischio associati alla devianza criminale. La predizione del *risk assessment tool* si trova dunque a metà tra prova e valutazione: pur non essendo diretta alla dimostrazione del fatto-reato, questa incide in modo significativo sulla decisione del giudice rispetto al trattamento da applicare, sia esso di natura sanzionatoria o cautelare.

Di recente, peraltro, alcuni *risk assessment tools* sono stati incorporati in *software* predittivi

<sup>107</sup> Parlano di questo futuribile sviluppo VILLA ET AL. (2023).

<sup>108</sup> RYAN ET AL. (2024), pp. 14-26.

<sup>109</sup> BARONE (2024), p. 1058 nota infatti che la concentrazione delle trattative sul tema – politicamente polarizzato – della biometria ha oscurato totalmente gli altri possibili impieghi dell'IA nel settore giustizia.

<sup>110</sup> TONINI (2024), p. 248.

<sup>111</sup> Cfr., diffusamente, GLESS (2020), p. 222 nonché, per una prospettiva d'oltreoceano, CHESSMAN (2017). Rimane vero che lo stesso testimone esperto potrebbe non avere le informazioni necessarie a comprendere il perché della decisione del suo collaboratore digitale.

<sup>112</sup> UBERTIS (2024), p. 16.

<sup>113</sup> ZARA (2016), p. 7.

<sup>114</sup> GIALUZ (2019). In termini sostanzialmente analoghi QUATTROCOLO (2021b), p. 271.

del rischio di delinquenza,<sup>115</sup> che, partendo da un profilo personologico (composto da dati quali cittadinanza, luogo di nascita, luogo di residenza, il numero di figli, numero di precedenti condanne in sede giudiziaria), restituiscono il rischio di commissione di futuri delitti da parte del soggetto, indicandolo come un grado in un'apposita scala (ad es.: rischio alto, medio o basso). Non tutti i *software* che fanno *risk assessment* sono però IA. Il *software* spagnolo *VioGén*, per esempio, consiste semplicemente in un algoritmo programmato per predire la violenza di genere.<sup>116</sup> Al contrario, il sistema H.A.R.M. (*Harm Assessment Risk Tool*), sviluppato dalla polizia di Durham (Regno Unito), utilizza il *supervised machine learning* per classificare gli individui a seconda della probabilità che essi commettano crimini nei due anni successivi.<sup>117</sup>

Non è scontato, quindi, che i sistemi di *risk assessment* ricadano nell'ambito oggettivo di applicazione dell'AIA.

Il legislatore europeo annovera esplicitamente i *risk assessment tools* tra i sistemi vietati, qualora essi basino la predizione unicamente sulla profilazione<sup>118</sup> o sulla valutazione di caratteristiche della personalità (articolo 5(1) lett. d) AIA). Il divieto trova giustificazione nella violenza che una valutazione automatizzata – e, quindi, per natura meramente statistica – del rischio di recidiva userebbe al principio della presunzione di non colpevolezza.<sup>119</sup> L'interdizione sembra ad ampio spettro: la profilazione è la "linfa vitale" dei *risk assessment tools*, che su essa ordinariamente fondano le predizioni loro richieste.<sup>120</sup>

Nonostante il divieto, rimangono però due ampi bacini di operatività per i sistemi di *risk assessment*: da un lato vi sono i casi in cui il *tool* effettui la predizione sulla base di elementi diversi da quelli espressamente interdetti dal regolamento (la profilazione o la valutazione di tratti della personalità); dall'altro, l'art. 5(1), lett. d) AIA consente una deroga al divieto per taluni modelli, nei termini di cui a breve si dirà.

Quanto al primo caso, il legislatore esplicita, al considerando n. 42, quali IA vuole permettere: si tratta dei *software* impiegati nella valutazione il rischio di frode finanziaria da parte delle imprese sulla base di transazioni sospette. Ed invero, tali sistemi non si basano sulla profilazione, né valutano caratteristiche di persone fisiche.

La seconda ipotesi – l'eccezione stabilita dall'art. 5(1), lett. d) AIA – si riferisce ai modelli che, pur facendo uso delle risorse espressamente vietate in via generale, siano impiegati esclusivamente «a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa», a condizione che tale valutazione si fondi su «fatti oggettivi e verificabili».

La formulazione dell'eccezione è infelice. Il *risk assessment tool*, per definizione, non è «macchina retrospettiva»<sup>121</sup>, ma prospettiva: oggetto dell'*assessment* non è il coinvolgimento nel reato ma il rischio di recidiva.<sup>122</sup> Eppure, il regolamento si riferisce a sistemi che valutano comportamenti passati (il «coinvolgimento» in attività criminose). Proprio in ragione di tale *qui pro quo* linguistico parte della dottrina ha ritenuto che l'eccezione nemmeno si riferisca a sistemi di *risk assessment*, quanto piuttosto a metodiche di informatica forense, quelle si impiegabili per la valutazione del coinvolgimento nel reato.<sup>123</sup> Tuttavia, il considerando n. 42<sup>124</sup> rende chiaro che il sospetto non è l'oggetto della valutazione algoritmica, quanto piuttosto una sua ineluttabile premessa, legittimante il ricorso allo strumento predittivo. L'eccezione assume, così, una portata molto ampia, tanto da svuotare di contenuto il divieto generale imposto dal primo alinea dell'art. 5(1)(d) AIA.<sup>125</sup>

<sup>115</sup> Di per sé, l'espressione *risk assessment tool* è generica e non individua necessariamente uno strumento digitale, né tanto meno un sistema di IA. Si rimanda a QUATTROCOLO (2021b) p. 273 per una storia dell'evoluzione di questi *tools*.

<sup>116</sup> Ma vi sono già studi che applicano il *machine learning* ai dati di *VioGén*, v. GONZÁLEZ-PRIETO ET AL. (2022).

<sup>117</sup> British Centre for Data Ethics and Innovation (CDEI), *Review into bias in algorithmic decision-making*, 2020, p. 67.

<sup>118</sup> A norma dell'art. 3 n. 52) AIA, per profilazione si deve intendere «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» (art. 4, punto 4), reg. 2016/679).

<sup>119</sup> La *ratio* del divieto è illustrata al considerando n. 42 AIA, per cui v. oltre. Cfr., sul tema, GALGANI (2020), p. 86 e la dottrina ivi citata.

<sup>120</sup> QUATTROCOLO (2025), p. 6.

<sup>121</sup> L'espressione, riferita al processo, è sempre di CORDERO (2012), p. 568.

<sup>122</sup> A meno di non includere nel concetto di «valutazione del coinvolgimento in un'attività criminosa» anche quella relativa al trattamento sanzionatorio da applicare. Un'interpretazione inammissibile per via della sua estensione.

<sup>123</sup> Per questa opinione cfr. QUATTROCOLO (2025). Si può ribattere che, nonostante l'innegabile pasticcio linguistico, l'eccezione faccia comunque riferimento a sistemi di *risk assessment*, quantomeno *ratione loci*.

<sup>124</sup> A norma del quale le persone fisiche non dovrebbero mai essere giudicate sulla base di un comportamento previsto dall'IA basandosi unicamente sulla profilazione «senza che vi sia un ragionevole sospetto di coinvolgimento nelle attività criminose».

<sup>125</sup> A conferma dell'ampia portata dell'eccezione di cui all'art. 5(1) lett. d) AIA, le già citate linee guida della Commissione sulle pratiche vietate riportano esempi di pratiche ammissibili di utilizzo dei *risk assessment tools* in cui gli stessi non valutano propriamente il coinvolgimento delle

Una volta chiarito che l'AIA lascia largo spazio all'impiego dei *risk assessment tools*, bisogna chiedersi se essi debbano essere classificati come ad alto rischio. Come opportunamente sottolineato dalla Commissione Europea nelle proprie linee guida in materia di pratiche vietate,<sup>126</sup> la risposta dovrebbe essere positiva per tutti i sistemi ammessi. L'allegato III, par. 6, lett. d) AIA considera infatti come ad alto rischio, da un lato, gli strumenti di *risk assessment* che non si fondano esclusivamente su tecniche di profilazione; dall'altro, quelli destinati a valutare tratti personologici o il comportamento criminale pregresso di persone fisiche o gruppi.<sup>127</sup> Sicché la quasi totalità delle IA che effettuano predizioni su persone fisiche — c.d. sistemi personologici — ove non attratti dal divieto assoluto di cui all'art. 5 AIA, sarà comunque considerato ad alto rischio. Al contrario, saranno esclusi dal regime rafforzato di conformità i *software* applicati alla valutazione del rischio di frode finanziaria, cui fa espresso riferimento il considerando n. 42 del regolamento.

## 4.5.2. Risk assessment tools nel diritto nazionale.

Pur non risultando, allo stato, applicazioni documentate dei sistemi di *risk assessment* nel contesto processuale italiano, non v'è dubbio che il loro potenziale campo d'impiego si profili vastissimo:<sup>128</sup> spiccano in particolare il supporto al giudice nella valutazione del rischio di recidiva in sede cautelare (art. 274, lett. c) c.p.p.), della meritevolezza di misure alternative alla detenzione (v. ora il riformato art. 545-*bis* c.p.p.) o del beneficio della sospensione condizionale della pena (art. 164 c.p.), nonché nella fase esecutiva in senso ampio. In tutte le ipotesi richiamate, il sistema di *risk assessment* verrebbe in rilievo quale ausilio tecnico alla valutazione giudiziale, innestandosi su una prognosi che, sinora, ha trovato la propria cifra nell'intuizione del giudice, piuttosto che in una lettura oggettiva delle correlazioni statistiche tra caratteristiche personali del reo e propensione criminosa.

Quanto alle possibili modalità di ingresso nel procedimento degli *output* algoritmici generati da questa tipologia di sistemi, in dottrina si registrano, in via tendenziale, due principali linee ricostruttive.<sup>129</sup>

Alcuni autori hanno efficacemente messo in luce la prossimità funzionale tra le operazioni svolte dai programmi di *risk assessment* e la perizia c.d. personologica sulla tendenza a delinquere, oggetto di espresso divieto *ex* art. 220, comma II, c.p.p., ove non finalizzata all'esecuzione della pena o della misura di sicurezza.<sup>130</sup> A sostegno della tesi dell'assimilabilità, si richiama la *ratio* del divieto codicistico, che vuole salvaguardare tanto la presunzione di innocenza dell'imputato quanto la sua libertà morale.<sup>131</sup> Esigenza, questa, perfettamente sovrapponibile a quella sottesa al divieto previsto dall'art. 5(1), lett. d), AIA.<sup>132</sup>

Muovendo da tale impostazione, che qualifica i *risk assessment tools* alla stregua di accertamenti peritali, ne deriverebbe l'inammissibilità in sede cautelare e in fase di determinazione della pena. Una conclusione che risulta, sul piano applicativo, ancor più restrittiva rispetto alle condizioni imposte dall'AIA.<sup>133</sup>

Sul lato opposto, v'è chi tende a escludere l'applicabilità dello statuto della perizia, non essendo i *risk assessment tools* specificamente finalizzati a scandagliare la sfera interiore del prevenuto per dedurne il carattere, la personalità e in genere le sue qualità psichiche.<sup>134</sup> Secondo questa medesima dottrina, sarebbe illogico, peraltro, precludere l'ingresso dei sistemi di *risk*

persone nelle attività criminose, v. *Commission guidelines*, cit., p. 74.

<sup>126</sup> *Commission guidelines*, cit., p. 65, *sub* par. (185). Cfr. anche p. 70, *sub* par. (204).

<sup>127</sup> La rottura della complementarità con il divieto stabilito dall'art. 5(1)(d) AIA è evidente: vengono infatti classificati come ad alto rischio i sistemi «per valutare» i tratti e le caratteristiche della personalità (non più, come nel divieto, «basati sulla valutazione di caratteristiche della personalità»). In altri termini, l'apprezzamento personologico qui non è più mezzo ma fine. Non è dato sapere quanto la formulazione appena descritta sia intenzionale o frutto di uno sfortunato bisticcio linguistico dalle sfumature paradossali, accuratamente illustrate da QUATTROCOLO (2025), p. 7.

<sup>128</sup> Per l'elenco completo dei possibili utilizzi cfr. MAUGERI (2021), p. 2. V. anche MALDONATO (2022), p. 8; QUATTROCOLO (2021b), p. 259.

<sup>129</sup> Le riporta GUIDO (2023), p. 11, con riferimento ai sistemi usati in sede cautelare.

<sup>130</sup> Cfr. ad es. QUATTROCOLO (2025), p. 6. V. anche GALGANI (2020), p. 86 e la dottrina ivi citata.

<sup>131</sup> Cfr. Cass. pen., sez. I, 28 giugno 2006, n. 30402.

<sup>132</sup> V. ancora il considerando n. 42 AIA: «in linea con la presunzione di innocenza, le persone fisiche nell'Unione dovrebbero sempre essere giudicate in base al loro comportamento effettivo».

<sup>133</sup> Le *Guidelines* della Commissione sulle attività vietate dall'AIA, seppure, ancora, in via provvisoria, citano numerose modalità d'impiego di *risk assessment tools* anche in fase cautelare. V. *Commission guidelines*, cit. p. 65, *sub* par. (185). Cfr. anche p. 70, *sub* par. (214).

<sup>134</sup> *Inter alios* GIALUZ (2019), p. 20.

*assessment tools* in base a una disposizione – il 220, c. II c.p.p. – inserita nel codice in ragione dell'ideologica sfiducia del legislatore nei confronti della scienza criminologica, presuntivamente giudicata meno attendibile dell'intuito del giudice.<sup>135</sup>

Al di là dello scopo perseguito direttamente o indirettamente dai *risk assessment tools*, sono ragioni eminentemente pratiche che spingono a dubitare che gli stessi verranno categorizzati quali surrogati digitali di una perizia sulla capacità a delinquere del reo e, quindi, saranno in grado di attivare le relative formalità procedurali.

Verosimilmente, infatti, il *risk assessment tool* italiano sarà un *software* sviluppato dal (o per conto del) Ministero della Giustizia o dell'Interno e messo a disposizione delle amministrazioni penitenziarie o dell'ufficio per l'esecuzione penale esterna. Guardando oltreoceano, le valutazioni compiute dai *risk assessment tools* entrano nella cognizione dei giudici attraverso intermediari: nel celebre caso *Loomis*, ad esempio, il giudice ordinò una *presentence investigation* prima di procedere al *sentencing*. Il *presentence investigation report* ("PSI") inoltrato dagli ufficiali competenti (i c.d. *probation and parole officers*)<sup>136</sup> includeva proprio l'esito algoritmico del sistema COMPAS.<sup>137</sup> È evidente, dunque, che lo strumento di predizione del rischio viene concepito, in quel sistema, come uno strumento di corredo a una più ampia valutazione degli addetti dell'amministrazione penitenziaria. L'*output* algoritmico, in altre parole, fornisce al ragionamento del giudice una base statistica, e non invece la «conoscenza» (*knowledge*) scientifica o tecnica di un esperto, come richiesto dall'art. 702 delle *federal rules of evidence* per la «*expert testimony*»<sup>138</sup>.

Il nostro ordinamento – che invero disconosce una così netta distinzione tra la fase di accertamento della responsabilità e quella di *sentencing*<sup>139</sup> – già consente al giudice, ai sensi dell'art. 236 c.p.p., di acquisire elementi relativi alla personalità dell'imputato, attraverso l'accesso al casellario giudiziale, alla documentazione esistente presso i servizi sociali degli enti pubblici e gli uffici di sorveglianza, nonché alle sentenze irrevocabili (art. 236 c.p.p.). La giurisprudenza<sup>140</sup> e la dottrina maggioritaria<sup>141</sup> peraltro negano la tassatività dell'elencazione.

Ci si troverà quindi realisticamente di fronte a una prova precostituita, un documento incorporante una valutazione algoritmica sul rischio di delinquenza. La questione, allora, non sarà tanto quella del rispetto della libertà morale dell'imputato, quanto piuttosto quella del rispetto del contraddittorio nella formazione della prova, principio che l'art. 236 c.p.p. neanche troppo surrettiziamente aggira.<sup>142</sup> In questo caso, l'assenza di un dibattito tecnico precluderebbe qualsiasi possibilità di verifica sul metodo di formazione del documento; *a fortiori*, verrebbe meno ogni possibilità di accertare la conformità ai requisiti elaborati dalla giurisprudenza di legittimità in materia di prove a contenuto tecnico-scientifico.<sup>143</sup>

All'eccezione della difesa sul punto, la Procura potrà tuttavia replicare che dalla classificazione dei *risk assessment tools* (di natura personologica) come sistemi IA ad alto rischio discende una nutrita serie di obblighi di *compliance*, anche e soprattutto in termini di qualità dei dati di *training* e di affidabilità.<sup>144</sup> I rischi di discriminazione razziale spesso paventati in merito all'utilizzo dei sistemi in esame dovrebbero dunque essere d'un lato esposti nella documentazione tecnica del sistema, da un altro mitigati *ex ante* attraverso l'allenamento con dati sufficientemente rappresentativi.

L'*assessment report*, creato secondo i canoni di scientificità imposti dall'AIA e dalla relativa regolamentazione di attuazione, dovrà infine essere prudentemente rimesso alla valutazione del giudice, che dovrà riconoscerne la natura essenzialmente probabilistica.<sup>145</sup> Chissà che il supporto *data-driven* offerto dal sistema non finisca per stanare pregiudizi e moti emozionali

<sup>135</sup> *Ibidem*.

<sup>136</sup> HANSER (2013), p. 54.

<sup>137</sup> *Loomis v. Wisconsin*, 881 N.W.2d 749 (Wis. 2016), p. 6.

<sup>138</sup> Rimane controverso se le IA debbano rispettare i criteri di scientificità enunciati negli Stati Uniti nella sentenza che ha anticipato la Cassazione *Cozzini*, ovvero *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993). V. sul punto CONTISSA ET AL. (2019), p. 623. In un caso del 2024 la *Superior Court Of Washington For King County* ha richiesto il rispetto della *rule of evidence* n. 401 in un caso relativo a un *software* di elaborazione digitale dei video, il *Topaz Video AI*, v. *State Of Washington v. Joshua Puloka*, no. 21-1-04851-2 KNT, 29 marzo 2024.

<sup>139</sup> GALGANI (2020), p. 82.

<sup>140</sup> Cass. pen. sez. II, 5 maggio 2010, n. 18189 sull'acquisizione dei dati contenuti nell'archivio informatico della polizia di Stato; sez. V, 21 ottobre 2019 n. 9106 sempre con riferimento ai precedenti di polizia; sez. VI del 29 marzo 2012, n. 22274 in relazione ai rilievi dattiloscopici.

<sup>141</sup> CANTONE (2004), p. 79; SQUASSONI (1990), p. 652; *Contra* UBERTIS (1992), p. 2516.

<sup>142</sup> Vi si riferisce GALGANI (2020), p. 83.

<sup>143</sup> Il riferimento è a Cass. pen., sez. IV, 17 settembre 2010, n. 43786, *Cozzini*. Sul tema, v. QUATTROCOLO (2021b), p. 280.

<sup>144</sup> GALGANI (2020), p. 85.

<sup>145</sup> MALDONATO (2022), p. 10.

che, ad oggi, continuano a esercitare un ruolo sotterraneo ma determinante nella giustizia preventiva e non solo.<sup>146</sup>

## 5.

### L'IA come mero supporto del giudice e delle parti.

Da ultimo, meritano attenzione i sistemi destinati a svolgere una funzione meramente ausiliaria rispetto all'attività dell'autorità giudiziaria o delle parti. Si tratta, ad esempio, dei *software* specifici per l'analisi di testi normativi e della giurisprudenza (quando non per la scrittura di bozze di provvedimenti e atti). La categoria, quindi, non comprende i sistemi c.d. generalisti (come *ChatGPT* o *Copilot*) che vengono *anche* utilizzati per fini di ricerca giuridica.<sup>147</sup>

L'allegato III, n. 8, lett. a) AIA qualifica come ad alto rischio le IA impiegate da un'autorità giudiziaria, o per suo conto, per assisterla nella ricostruzione e interpretazione dei fatti e del diritto, nonché nell'applicazione della legge a una fattispecie concreta. La disposizione non è di facile interpretazione.

*In primis*, da un punto di vista sistematico, la formulazione appare tanto ampia da ricomprendere pressoché ogni applicazione dell'IA nel processo, comprese quelle già esaminate nei paragrafi precedenti. In effetti, qualunque sistema che elabori *input* rilevanti ai fini processuali può, in senso lato, dirsi "di assistenza" all'autorità giudiziaria. Nel rispetto del criterio della *lex specialis*, dunque, la norma dovrà essere letta in chiave restrittiva, attribuendo centralità al verbo «assistere», da intendersi quale mera attività di supporto materiale e non decisionale.

*In secundis*, la disposizione in parola sembra circoscrivere il proprio ambito soggettivo alle IA impiegate dall'«autorità giudiziaria», espressione che parrebbe escludere le difese, anche di parte civile.

Sul fronte nazionale, la l. 23 settembre 2025, n. 132 ammette all'art. 15 l'uso dell'IA nell'attività giudiziaria: i sistemi del Ministero semplificheranno non solo l'organizzazione dei servizi alla giustizia e le «attività accessorie»<sup>148</sup>, ma anche il lavoro dei magistrati. La nuova normativa, però, riserva alla giurisdizione «umana» «ogni decisione sull'interpretazione e applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti», con ciò di fatto ammettendo l'uso dell'IA nelle attività diverse da quelle esplicitamente menzionate.

In attesa delle prime mosse del Ministero in questo settore, già si riconosce quale sarà la vera sfida: imporre — quantomeno al pubblico ministero e al giudice — l'impiego di sistemi espressamente concepiti per l'assistenza giuridica, conformi ai requisiti di trasparenza, tracciabilità e affidabilità richiesti dal regolamento per i sistemi ad alto rischio. In difetto di una simile cautela, si corre il rischio concreto che gli operatori del diritto si affidino a sistemi c.d. *general purpose* (come *ChatGPT*) di più agevole accesso ma privi di una progettazione mirata a supportare le funzioni dell'autorità giudiziaria e, soprattutto, slegati dagli obblighi gravanti sui sistemi ad alto rischio.<sup>149</sup> Sul piano difensivo soccorreranno, al medesimo scopo, le normative d'origine ordinistica.<sup>150</sup>

## 6.

### Riflessioni conclusive.

L'AIA si distingue per una struttura complessa, scandita da divieti ed eccezioni, che certo non concorre a delineare un quadro normativo limpido. Le categorie adottate, spesso prive di definizioni stabilizzate sul piano scientifico, si devono peraltro misurare con contesti nazionali profondamente disomogenei, tanto nelle prassi quanto nelle architetture previste per l'impie-

<sup>146</sup> CAIANIELLO (2021), p. 14.

<sup>147</sup> Si tratta di sistemi «per finalità generali», che trovano nell'AIA una disciplina specifica, v. artt. 51 ss. AIA.

<sup>148</sup> Art. 15, c. II, l. cit.: «Il Ministero della giustizia disciplina gli impieghi dei sistemi di intelligenza artificiale per l'organizzazione dei servizi relativi alla giustizia, per la semplificazione del lavoro giudiziario e per le attività amministrative accessorie».

<sup>149</sup> E, quindi, a più alto rischio di «allucinazione», v. Trib. Imprese Firenze, ordinanza del 14 marzo 2025 in tema di sentenze inesistenti generate da *ChatGPT*.

<sup>150</sup> Vedi ad es. la *Carta dei Principi per un Uso Consapevole dei Sistemi di Intelligenza Artificiale in Ambito Forense* dell'Ordine degli Avvocati di Milano, gennaio 2025. In tema, l'art. 13, c. I, l. 132/2025 dispone che: «l'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è finalizzato al solo esercizio delle attività strumentali e di supporto all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera».

go delle IA.

Purtuttavia il regolamento, trattando l'IA essenzialmente alla stregua di un prodotto, introduce una logica di standardizzazione tecnica di sistemi che saranno impiegati nei procedimenti penali europei. La nascita, anche per i sistemi utilizzati nella giustizia penale, di criteri comuni in materia di trasparenza, tracciabilità, supervisione e qualità dei dati genera un'eternità positiva di rilievo sistemico. Sconfessandone l'*habitus* di mero strumento ausiliario alle indagini, l'innalzamento dei requisiti tecnici chiarisce la natura scientifica delle IA "penalistiche", imponendone l'impiego nei modi dell'accertamento tecnico.

In questa prospettiva, il livello effettivo di garanzie poste in caso di esposizione all'IA nei procedimenti penali dipenderà essenzialmente da due fattori. Innanzitutto, dalla serietà della *compliance*, che nel settore del *law enforcement* conserva purtroppo elevatissimi margini di autodisciplina. Ma anche, e soprattutto, dalla capacità del processo penale italiano di metabolizzare questa nuova forma di prova tecnica, evitando che i *report* algoritmici finiscano per dilatare quella zona grigia in cui documenti nati fuori dal processo ottengono dignità decisoria.

Vale ancora, e lo si deve ricordare, il rilievo secondo cui la prova scientifica non costituisce un'eccezione metodologica, ma si sottopone — al pari di ogni altra — al vaglio del contraddittorio e alla regola del ragionevole dubbio.<sup>151</sup> Solo attraverso la valorizzazione piena di questo canone sarà possibile garantire che la tecnologia, pur nel suo potenziale di innovazione, resti ancillare rispetto alla legalità del giudizio. Andrebbe dunque valorizzata la ripetibilità che, nella quasi totalità dei casi, connota le operazioni algoritmiche dell'IA operate in fase d'indagine, così da consentire una rinnovazione in dibattito dell'analisi, nel perimetro di un contraddittorio tecnico ispirato ai canoni di scientificità ormai solidamente accolti nel nostro ordinamento.

In altre parole, solo attraverso una rigorosa attenzione al metodo sarà possibile cogliere gli indubbi benefici dell'intelligenza artificiale «utile» al processo penale,<sup>152</sup> scongiurando al contempo i rischi a essa connessi.

## Bibliografia

BARONE, Giulia (2024): "Artificial Intelligence Act: un primo sguardo al regolamento che verrà", *Cassazione penale*, 3, pp. 1047 ss.

BENANTI, Paolo (2024): "Perché bisogna parlare di 'intelligenze artificiali'", *Nuova Atlantide*, 11

CAIANIELLO, Michele (2012): *Premesse per una teoria del pregiudizio effettivo nelle invalidità processuali penali* (Bologna, Bononia University Press)

CAIANIELLO, Michele (2018): "L'ammissione della prova scientifica nel processo italiano", in CANZIO, Giovanni e LUPARIA, Luca: *Prova scientifica e processo penale* (Padova, Cedam)

CAIANIELLO, Michele (2021): "Dangerous liaisons. Potentialities and risks deriving from the interaction between artificial intelligence and preventive justice", *European Journal of Criminal Justice*, 29, pp. 1 ss.

CALIGIORE, Daniele (2024): *Curarsi con l'intelligenza artificiale* (Bologna, Il Mulino)

CAMON, Alberto ET AL. (2023): *Fondamenti di procedura penale* (Padova, Cedam)

CANTONE, Raffaele (2004): *La prova documentale* (Milano, Giuffrè)

CANZIO, Giovanni (2022): "Intelligenza artificiale e processo penale", in CANZIO, Giovanni e LUPARIA, Luca (a cura di): *Prova scientifica e processo penale* (Padova, Cedam)

CAPRIOLI, Francesco (2008): "La scienza 'cattiva maestra': le insidie della prova scientifica nel processo penale", *Cassazione penale*, 9, pp. 3520 ss.

<sup>151</sup> CAIANIELLO (2018), p. 203.

<sup>152</sup> QUATTROCOLO (2021a), pp. 387 ss.

CASONATO, Carlo e MARCHETTI, Barbara (2021): “Prime osservazioni sulla proposta di regolamento dell’Unione Europea in materia di intelligenza artificiale”, *BioLaw Journal – Rivista di BioDiritto*, 3, pp. 415-437

CHESSMAN, Christian (2017): “A ‘source’ of error: computer code, criminal defendants, and the Constitution”, *California Law Review*, 105

CONTISSA, Giuseppe ET AL. (2019): “Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo”, *Diritto di Internet*, 4, pp. 619 ss.

CORDERO, Franco (1992): *Codice di procedura penale commentato* (Torino, UTET)

CORDERO, Franco (2012): *Procedura penale* (Milano, Giuffrè), p. 572

della torre, Jacopo (2020): “Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della *High Court of Justice*”, *Rivista Trimestrale di Diritto Penale Contemporaneo*, 1, pp. 231 ss.

DELLA TORRE, Jacopo (2022): “Quale spazio per i *tools* di riconoscimento facciale nella giustizia penale?”, in DI PAOLO, Gabriella e PRESSACCO, Luca (a cura di): *Intelligenza Artificiale e processo penale. Indagini, prove, giudizio* (Napoli, Editoriale Scientifica), pp. 7 ss.

DINACCI, Filippo Raffaele (2023): “L’inutilizzabilità e il *male captum bene retentum*: vecchie superstizioni e nuove consapevolezze”, *Archivio Penale Web*, 2

DOMINIONI, Oreste (2005): *La prova penale scientifica* (Milano, Giuffrè)

DONATI, Filippo (2025): “La protezione dei diritti fondamentali nel regolamento sull’intelligenza artificiale”, *Rivista AIC*, 1

ESPOSITO, Elenia (2024): “Nuovi strumenti di lotta all’illegalità, riflessioni nell’era dell’intelligenza artificiale”, *Penale Diritto e Procedura*, 2 ottobre

FERRUA, Paolo (2024): “Franco Cordero e il processo accusatorio”, *Teoria e Critica della Regolazione Sociale*, 1, pp. 9 ss.

FLORIDI, Luciano (2014): *The fourth revolution: how the infosphere is reshaping human reality* (Oxford, Oxford University Press)

GALANTINI, Novella (1997): “Inutilizzabilità (Diritto e Processo Penale)”, in AA. VV.: *Enciclopedia del Diritto* (Milano, Giuffrè)

GALGANI, Benedetta (2020): “Considerazioni sui ‘precedenti’ dell’imputato e del giudice al cospetto dell’IA nel processo penale”, *Sistema Penale*, 4, pp. 81 ss.

GARRETT, Brandon (2023): “*The right to a glass box: rethinking the use of artificial intelligence in criminal justice*”, *Duke Law School Public Law & Legal Theory Series*, 3

GARRETT, Brandon e RUDIN, Cynthia (2024): “Testing AI”, disponibile su SSRN al link: [www.ssrn.com/abstract=4948789](https://www.ssrn.com/abstract=4948789)

GENNARI, Giuseppe (2016): *Nuove e vecchie scienze forensi alla prova delle corti. Un confronto internazionale e una proposta per il futuro* (Santarcangelo di Romagna, Maggioli Editore)

GIALUZ, Mitja (2019): “Quando la giustizia penale incontra l’intelligenza artificiale: luci e ombre dei *risk assessment tools* tra Stati Uniti ed Europa”, *Diritto Penale Contemporaneo*, 29 maggio

GIALUZ, Mitja (2021): “Intelligenza artificiale e diritti fondamentali in ambito probatorio”, in AA. VV.: *Giurisdizione penale, intelligenza artificiale ed etica di giudizio* (Milano, Giuffrè)

GIALUZ, Mitja (2025): “Prove fondate sull’intelligenza artificiale e diritti fondamentali”, *Diritto di Difesa*, 15 gennaio

- GIALUZ, Mitja e QUATTROCOLO, Serena (2023): “*AI And the Administration of Criminal Justice in Italy*”, *atti dell’AIDP*
- GLESS, Sabine (2020): “*AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials*”, *Georgetown Journal of International Law*, 51, pp. 195 ss.
- GONZÁLEZ-PRIETO, Ángel ET AL. (2022): “*Hybrid machine learning methods for risk assessment in gender-based crime*”, *Knowledge-Based Systems*, 260
- GRIFANTINI, Fabio Maria (2005): in CONSO, Giovanni e GREVI, Vittorio (a cura di): *Commentario breve al codice di procedura penale* (Padova, Cedam), sub art. 188
- GUIDO, Elisabetta (2023): “Intelligenza artificiale e procedimento penale: ragionando di valutazione del rischio *de libertate*”, *Archivio penale*, 1, pp. 1 ss.
- HANSER, Robert (2013): *Community Corrections* (New York)
- JELOVCICH, Martina (2014): “L’impiego di tecnologie biometriche nel procedimento penale”, *Diritto penale contemporaneo*
- LASAGNI, Giulia (2022): “Difendersi dall’intelligenza artificiale o difendersi con l’intelligenza artificiale? Verso un cambio di paradigma”, in DI PAOLO, Gabriella e PRESSACCO, Luca (a cura di): *Intelligenza Artificiale e processo penale. Indagini, prove, giudizio* (Napoli, Editoriale Scientifica)
- LOPEZ, Rita (2019): “La rappresentazione facciale tramite software”, in SCALFATI, Adolfo (a cura di): *Le indagini atipiche* (Torino, Giappichelli), pp. 248 ss.
- LORUSSO, Sergio (2009): “La prova scientifica”, in AA. Vv.: *Prova penale e metodo scientifico* (Torino, UTET)
- LUPARIA DONATI, Luca (2006): *La confessione dell’imputato nel sistema processuale penale* (Milano, Giuffrè)
- MALDONATO, Lucia (2022): “*Risk and need assessment tools* e riforma del sistema sanzionatorio: strategie collaborative e nuove prospettive”, *Discrimen*, 18 ottobre
- MARANDOLA, Antonella (2023): “Il riconoscimento facciale”, in CONTI, Carlotta e MARANDOLA, Antonella (a cura di): *La prova scientifica* (Milano, Giuffrè), pp. 495 ss.
- MARCHETTI, Barbara (2024): “La regolazione europea del mercato dell’intelligenza artificiale”, *Rivista della Regolazione dei Mercati*, 1
- MAZZARELLI, Claudio (a cura di) (2000): *Aristotele. Etica Nicomachea* (Milano, Bompiani)
- MOLARI, Alessandro (2002): “Introduzione alla tavola rotonda”, in AA. Vv. (a cura di): *Il contraddittorio tra Costituzione e legge ordinaria. Atti del convegno organizzato dall’Associazione tra gli studiosi del processo penale* (Milano, Giuffrè), pp. 137 ss.
- NOBILI, Massimo (1990a) in CHIAVARIO, Mario (a cura di): *Commento al codice di procedura penale*, sub art. 189, tomo II
- NOBILI, Massimo (1990b) in CHIAVARIO, Mario (a cura di): *Commento al codice di procedura penale*, sub art. 191, tomo II
- NOVELLI, Claudio (2024): “*L’Artificial Intelligence Act* europeo: questioni di implementazione”, *Federalismi.it*, 2
- NOVELLI, Claudio ET AL. (2024): “*AI risk assessment: a scenario-based, proportional methodology for the AI Act*”, *Digital Society*, 3 (13)
- PALMIOTTO, Francesca (2023): *Artificial intelligence and the transformation of criminal trials: preserving fairness in Europe*, tesi dottorale (Firenze)

PANZAVOLTA, Michele e MAES, Elise (2022): “*Exclusion of evidence in times of mass surveillance. In search of a principled approach to exclusion of illegally obtained evidence in criminal cases in the European Union*”, *International Journal of Evidence & Proof*, 26 (3), pp. 199 ss.

PASSALACQUA, Giovanni (2020): “Ricognizione e brevi considerazioni in materia di criteri di valutazione della prova indiretta nel giudizio cautelare”, *Penale Diritto e Procedura*, 12 giugno

PICCININI, Andrea e GENNARI, Giuseppe (2021): *La prova del DNA. Istruzioni per il giurista* (Santarcangelo di Romagna, Maggioli Editore)

PIETROCARLO, Elisabetta (2024): “La *predictive policing* nel regolamento europeo sull’intelligenza artificiale”, *La Legislazione Penale*, 26 settembre

PRESSACCO, Luca (2022): “Intelligenza artificiale e ragionamento probatorio nel processo penale”, in DI PAOLO, Gabriella e PRESSACCO, Luca (a cura di) (2022): *Intelligenza Artificiale e Processo Penale. Indagini, Prove, Giudizio* (Napoli, Editoriale Scientifica), pp. 91 ss.

QUATTROCOLO, Serena (2020): *Artificial intelligence, computational modelling and criminal proceedings. a framework for a european legal discussion* (Cham, Springer)

QUATTROCOLO, Serena (2021a): “Per un’intelligenza artificiale utile al giudizio penale”, *rivista BioDiritto*, 2, pp. 387 ss.

QUATTROCOLO, Serena (2021b): “Sui rapporti tra pena, prevenzione del reato e prova nell’era dei modelli computazionali psico-criminologici”, *Teoria e Critica della Regolazione Sociale*, 1

QUATTROCOLO, Serena (2023): “Prova e intelligenza artificiale”, in CONTI, Carlotta e MARANDOLA, Antonella (a cura di): *La prova scientifica* (Milano, Giuffrè)

QUATTROCOLO, Serena (2025): “Intelligenza artificiale e processo penale: le novità dell’*AI Act*”, *Diritto di Difesa*, 16 gennaio

RAJS, Nora ET AL. (2025): “*Determining time since deposition of latent fingerprints on forensic adhesive tape using ultrafast DESI-MS and machine learning*”, *Scientific Reports*, 15

RYAN, Shannon ET AL. (2024): “*Machine learning for predicting the outcome of terminal ballistics events*”, *Defence Technology*, 31, pp. 14-26

SACCHETTO, Ernestina (2020): “*Face to Face: il Complesso Rapporto tra Automated Facial Recognition Technology e Processo Penale*”, *Legislazione Penale*

SACCHETTO, Ernestina (2022): “Riconoscimento facciale, l’approccio italiano è in antitesi alla Ue: i nodi”, *Agenda Digitale*, 7 dicembre

SACCHETTO, Ernestina (2023): “La prova biometrica”, in CONTI, Carlotta e MARANDOLA, Antonella (a cura di): *La prova scientifica* (Milano, Giuffrè)

SQUASSONI, Claudia (1990) in CHIAVARIO, Mario (a cura di): *Commento al codice di procedura penale*, sub art. 236, tomo II

SUNDE, Inger Marie (2022): “*AI-based Law Enforcement Online: The Impact of the European Artificial Intelligence Act (AIA)*”, *Bergen Journal of Criminal Law and Criminal Justice*, 2/10, pp. 29 ss.

TONINI, Paolo (2024): *Manuale di procedura penale* (Milano, Giuffrè)

UBERTIS, Giulio (1992): “Variazioni sul tema dei documenti”, *Cassazione penale*, pp. 2516 ss.

UBERTIS, Giulio (2024): “Perizia, prova scientifica e intelligenza artificiale nel processo penale”, *Sistema Penale*, 2 giugno

UCHIDA, Craig (2009): “A national discussion on predictive policing: defining our terms and mapping successful implementation strategies”, *National Institute of Justice*

VILLA, Chiara ET AL. (2023): “A virtual, 3D multimodal approach to victim and crime scene reconstruction”, *Diagnostics*, 13

ZARA, Georgia (2016): *Valutare il rischio in ambito criminologico. Procedure e strumenti per l'assessment psicologico* (Bologna, Il Mulino)



Diritto Penale Contemporaneo

R I V I S T A   T R I M E S T R A L E

---

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

<http://dpc-rivista-trimestrale.criminaljusticenetwork.eu>