https://doi.org/10.60923/issn.1825-1927/22088 ISSN 1825-1927

L'informazione nelle investigazioni data driven

Tina Salerno [1] [2] [3] [4]

[1] IMT Alti Studi di Lucca

[2] Università di Bologna, Dipartimento di Scienze Giuridiche

[3] Università di Bologna, Dipartimento di Informatica, Scienza e Ingegneria

[4] University oF Wroclau, Justice Digital Center

Abstract: Il presente contributo esamina le nuove forme di sorveglianza pubblica abilitate dall'intelligenza artificiale, che ridefiniscono l'epistemologia e la normatività dell'azione investigativa. Attraverso tecniche predittive e analisi automatizzate di dati, la funzione di prevenzione penale assume una struttura proattiva e probabilistica, ponendo in tensione i principi di legalità, proporzionalità e trasparenza. Muovendo da una genealogia concettuale della sorveglianza, il lavoro analizza il passaggio da modelli disciplinari centralizzati a dispositivi reticolari e opachi. Particolare attenzione è dedicata al Regolamento europeo sull'intelligenza artificiale (AI Act), di cui si discutono le implicazioni sistemiche e le lacune regolative. Si propone infine una riconcettualizzazione della sorveglianza pubblica in chiave costituzionale, orientata alla tutela dei diritti fondamentali nello spazio digitale alla luce dei canoni elaborati dalla Commissione europea "Pega".

Keywords: Data-driven, Hacking by Enforcement, A.i. act, Cyber Investigation, Future of cybersecurity

1 Introduzione

La sorveglianza non è più solo un dispositivo di controllo: è divenuta un'infrastruttura invisibile e pervasiva che modella il rapporto tra potere, conoscenza e libertà. Nell'era digitale, il suo esercizio non avviene più unicamente attraverso l'osservazione diretta, ma mediante l'elaborazione automatizzata di dati, spesso raccolti in modo opaco e processati da sistemi algoritmici complessi. Da un punto di vista genealogico, è possibile individuare tre principali configurazioni storiche della sorveglianza[1]: una fase premoderna, in cui il sapere si organizza come strumento di dominio (esemplificata, ad esempio, dal Domesday Book); una fase moderna, segnata dalla razionalizzazione amministrativa e dalla disciplina interna (il Panopticon benthamiano[2], l' "esame" foucaultiano); infine una fase post-panottica, in cui la sorveglianza diventa reticolare, predittiva e distribuita, abilitata da tecnologie digitali e datafied environments [3].

tina.salerno2@unibo.it (Tina Salerno);

1. G. Ziccardi, Internet, controllo e libertà- trasparenza, sorveglianza e segreto nell'era tecnologica, Raffello cortina editore 2019; E. Johnson, Il terrore nazista. La Gestapo, gli ebrei e i tedeschi; Milano, Mondadori, 2001;

2. Il termine Panopticon si riferisce al modello architettonico ideato dal filosofo e giurista Jeremy Bentham nel 1791. Questo progetto prevedeva una struttura carceraria circolare con una torre centrale da cui un unico sorvegliante poteva osservare tutti i detenuti senza che questi sapessero se e quando fossero osservati. L'intento era quello di indurre i prigionieri a comportarsi in modo disciplinato, poiché la possibilità costante di essere controllati li avrebbe spinti a conformarsi alle regole. Michel Foucault ha ripreso questo concetto nel suo celebre saggio Sorvegliare e punire (1975), utilizzandolo come metafora del potere disciplinare che permea le società moderne.

3. Per maggiore approfondimento vedasi M. Foucault, Gli anormali, Corso al Collège de France, 1974\1975- 1999 Feltrinelli, 2000, p. 45 e ss.; G. Ziccardi, Il ricatto digitale, il Mulino – 4\2017; D. Lyon, Surveillance Studies, cit. pag. 73.

In questo contesto, l'adozione di strumenti investigativi data-driven rappresenta una vera svolta paradigmatica. Le tecniche di sorveglianza algoritmica, basate sull'elaborazione predittiva di dati eterogenei, si propongono di individuare pattern di rischio anche in assenza di indizi personalizzati, sollevando interrogativi profondi in termini di proporzionalità, trasparenza e tutela delle garanzie. A differenza dei modelli tradizionali di investigazione, questi strumenti trasformano la logica dell'intervento pubblico: da reattiva a proattiva, da personalizzata a probabilistica[4].

Il presente lavoro analizza criticamente tali pratiche, con particolare attenzione alle cyber-investigazioni in ambito europeo. L'adozione di questi strumenti configura una nuova forma di sorveglianza, algoritmica e opaca, che si discosta radicalmente dai modelli tradizionali fondati sulla discrezionalità controllata e sulla verificabilità dell'azione amministrativa. La natura statistica e probabilistica delle decisioni automatizzate, la difficoltà di attribuire responsabilità individuali, nonché l'impossibilità, per il cittadino, di comprendere — e dunque contestare — le logiche sottese ai processi decisionali, rendono problematico l'adattamento dei paradigmi giuridici esistenti.

Analizza, altresì, le implicazioni di questa trasformazione, concentrandosi in particolare su tre assi tematici: la crisi del paradigma classico della legalità nell'ambito della sorveglianza statale; le ambizioni e i limiti del nuovo Regolamento europeo sull'intelligenza artificiale (AI Act); e infine, le sfide poste dalla criminalità organizzata digitale e dalla crescente instabilità del quadro normativo in materia di prove informatiche. Attraverso un'analisi critica, orientata dai criteri di necessità, proporzionalità, trasparenza e non discriminazione elaborati dalla Commissione PEGA del Parlamento Europeo, il contributo intende mostrare come il ricorso all'I.A. in ambito investigativo, in assenza di solide garanzie giuridiche, rischi di produrre una deriva tecnocratica che compromette l'equilibrio tra innovazione e tutela dei diritti fondamentali.

Di fronte a un simile scenario, si impone la necessità di un ripensamento profondo delle categorie giuridiche tradizionali, volto a ricollocare la tecnologia entro i confini dello Stato di diritto. A partire da questa tripartizione, si argomenta che la cybersecurity non può essere ridotta a misura difensiva, ma deve essere riconosciuta come una condizione normativa per l'affidabilità epistemica delle prove digitali e per la legittimità delle indagini basate sull'uso di dati automatizzati. L'elaborato propone infine una riconcettualizzazione della sorveglianza pubblica in chiave costituzionalmente orientata: l'efficacia preventiva non può essere disgiunta dal rispetto di criteri rigorosi di legalità, trasparenza, necessità e proporzionalità, come richiesto dall'art. 8 della CEDU e dalla Carta dei Diritti Fondamentali dell'Unione Europea.

2 La sorveglianza pubblica tra crisi del principio di legalità e limiti dell'AI Act

2.1 Definizione e crisi del modello classico

Una riflessione giuridica adeguata sul fenomeno della sorveglianza pubblica impone, preliminarmente, una chiarificazione concettuale[5]. Secondo un'impostazione coerente con la teoria generale del diritto, può definirsi sistema pubblico di sorveglianza quell'insieme organizzato di strumenti e procedure volto a garantire l'ordine pubblico attraverso forme di monitoraggio preventivo, esercitate da autorità pubbliche e orientate alla gestione del rischio, nel rispetto — almeno teoricamente — dei diritti fondamentali della persona[6].

Questa definizione, che trova riscontro in una consolidata letteratura penalistica e criminologica, è oggi posta sotto pressione dall'emersione di nuove pratiche sorveglianza algoritmica, caratterizzate da un impiego massivo di dati e da una crescente dipendenza da strumenti tecnologici opachi, brevettati da attori privati e scarsamente sottoposti a controllo pubblico[7].

4. V. Aiuti, Epistemologia della sorveglianza, in Sicurezza, informazioni e giustizia penale, Scienze giuridiche della sicurezza, Pacini Giuridica, 2023

5. A. Vercellone, Sorveglianza, prevenzione e diritti fondamentali. Un'analisi comparata, Il Mulino, 2020;

6. A. Stanzione, L'era della sorveglianza: rischi e opportunità della società digitale, Giappichelli, 2021.

7. P. Pietrocarlo, Predictive policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali, in Rivista di Criminologia, Vittimologia e Sicurezza, 2018, n. 3.

2.2 Le forme attuali della sorveglianza pubblica

Tra i modelli più discussi vi è quello del predictive policing, basato sull'impiego di algoritmi per l'identificazione di hotspot del crimine e sulla costruzione di relazioni tra eventi, soggetti e contesti sulla base del linking crime[8]. Tale approccio si avvale di banche dati come il Sistema di Indagine (SDI), contenente informazioni su individui precedentemente coinvolti in attività criminali o legati a reti criminali attraverso relazioni sociali o familiari[9]. L'inserimento, in questi database, di dati relativi a soggetti privi di precedenti penali, o la semplice analisi delle loro connessioni sociali, solleva interrogativi fondamentali sul piano del diritto alla riservatezza e sulla tenuta del principio di non colpevolezza, oltre a compromettere la possibilità di reinserimento sociale di ex detenuti.

La giurisprudenza della Corte di cassazione ha chiaramente affermato che "la mera frequentazione di soggetti ritenuti di interesse investigativo non integra, di per sé, un presupposto idoneo a giustificare l'applicazione automatica o estensiva di misure limitative della libertà personale, in assenza di concreti e attuali elementi indiziari a carico del soggetto coinvolto"[10]. Si tratta di un monito rilevante, che richiama la necessità di distinguere la valutazione del rischio dalla attribuzione di responsabilità penale.

Già nel 1990, Renzo Orlandi identificava tre orientamenti teorici nella riflessione penalistica sull'irruzione del paradigma della sorveglianza nel processo penale: l'approccio remissivo, che prende atto dell'evoluzione tecnologica senza elaborare criteri normativi di contenimento; l'approccio costruttivo, che propone strumenti di regolazione orientati alla tutela dei diritti fondamentali; e infine l'approccio conservatore, che riafferma la priorità dei principi dello Stato di diritto rispetto a ogni istanza di efficienza investigativa[11].

Nell'attuale panorama europeo, diverse autorità investigative nazionali e sovranazionali fanno uso di tecnologie invasive per finalità di prevenzione e contrasto della criminalità[12]. In ambito italiano, tra le principali autorità pubbliche coinvolte figurano la Polizia di Stato, l'Arma dei Carabinieri, la Guardia di Finanza, nonché le Procure della Repubblica, coordinate dal Pubblico Ministero[13]. A livello sovranazionale, vanno segnalati attori quali Europol, in funzione di supporto analitico e tecnico alle autorità nazionali, e Eurojust, che agevola la cooperazione giudiziaria nel perseguimento dei reati transfrontalieri[14].

Tali soggetti si avvalgono, con frequenza crescente, di strumenti sviluppati da provider privati [15]— come spyware, sistemi di risk assessment predittivo, captatori informatici [16]e tecnologie di riconoscimento biometrico [17]— spesso in assenza di un controllo trasparente sui processi algoritmici sottostanti.

Oggi, l'evoluzione delle tecnologie digitali impone una nuova e più radicale interrogazione critica.

8. S. Quattrocolo, Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva", in Cassazione Penale, 2020, n. 10.

9. Sul principio di non colpevolezza e la sua tenuta di fronte a banche dati come il Sistema di Indagine (SDI), cfr. G. Spangher, Il principio di non colpevolezza, Giuffrè, 2018.

10. Cass. pen., Sez. V, 12 maggio 2022, n. 18991, ha ribadito che la mera frequentazione di soggetti di interesse investigativo non è sufficiente a giustificare l'applicazione di misure limitative della libertà personale.

11. R. Orlandi, Processo penale e trasformazioni sociali: il paradigma della sorveglianza, in Rivista Italiana di Diritto e Procedura Penale, 1990, n. 2.

12. P. Re, Polizia e tecnologie. Nuove frontiere della sorveglianza e del controllo sociale, Giappichelli, 2019.

13. M. C. R. Rota, L'impiego di nuove tecnologie investigative nel contrasto al terrorismo: profili di diritto comparato in Diritto Pubblico Comparato ed Europeo, 2017.

14. Europol, Internet Organised Crime Threat Assessment (IOCTA), Report annual 2024.

15. Sul punto, si segnala per maggiori approfondimenti: M.E Kaminski e G. Malgieri, Impacted stalkeholder partecipation in AI and Data Governance, Yale Journal of Law and Tecnology, Yale University, 2025.

16. Brighi Raffaella, *Requisiti tecnici, potenzialità e limiti del captatore informatico. Analisi sul piano informatico-forense*, in: Revisioni normative in tema di intercettazioni. Riservatezza, garanzie difensive e nuove tecnologie informatiche, Torino, Giappichelli, 2021, pp. 231 - 256 (PROCEDURA PENALE. COMMENTI) [capitolo di libro]; G. Castiglione, M. Maugeri, G. Bella, Detection of intrusion and malware, and vulnerability assessment, Spinger, 2025.

17. Per ulteriori approfondimenti, G. Fargetta, R. Zuccarà, A. Ortis, S. Battiato, "Exploiting adversarial learning and tipology augmentation for opern set visual recognition", CVPR25 , atti di convegno.

Il caso emblematico dello spyware Pegasus[18], utilizzato per monitorare giornalisti, attivisti e funzionari in vari contesti europei ed extraeuropei, ha evidenziato la vulnerabilità dell'individuo nei confronti di un potere investigativo che non conosce più limiti territoriali né garanzie procedurali[19]. La Commissione PEGA del Parlamento Europeo ha denunciato l'assenza di criteri di autorizzazione, controllo e supervisione adeguati e ha proposto una moratoria sull'utilizzo degli spyware da parte degli Stati membri. Un punto particolarmente problematico riguarda la possibilità, da parte di questi strumenti, di accedere in tempo reale a dati personali, localizzazione, comunicazioni cifrate e archivi personali, senza la collaborazione dei provider di telecomunicazione, infrangendo il principio di necessità e minando l'autonomia privata degli individui[20].

2.3 Tipologie di sorveglianza: verso un controllo sempre più pervasivo

Nell'ambito delle pratiche di sorveglianza intrusiva, è opportuno distinguere tra diverse tipologie di controllo, ciascuna delle quali comporta un differente livello di intrusività e una diversa tensione con i diritti fondamentali[21].

In primo luogo, si può parlare di sorveglianza ambientale generalizzata, come nel caso dei sistemi di videosorveglianza urbana, che operano in spazi pubblici e raccolgono dati in modo indiscriminato, spesso senza una finalità investigativa specifica. Una seconda forma, ben più pervasiva, è la sorveglianza digitale indiretta, fondata sull'analisi di dati di navigazione, metadati delle comunicazioni elettroniche, e pattern comportamentali, spesso ottenuti tramite data brokerage o cooperazione opaca con piattaforme digitali[22].

Vi è poi la sorveglianza mirata ad alta intrusività, come quella attuata attraverso spyware e captatori informatici, che permette l'accesso continuo e non notificato a dispositivi personali (smartphone, computer), incluse comunicazioni cifrate, posizione in tempo reale e contenuti archiviati[23]. Tali strumenti non si limitano alla raccolta passiva di dati, ma consentono un monitoraggio attivo e potenzialmente illimitato, spesso senza adeguate garanzie procedurali, come rilevato dalla Commissione PEGA[24].

Infine, si colloca una forma ibrida e crescente di sorveglianza predittiva, che combina dati massivi, tecniche di intelligenza artificiale e modelli di rischio per anticipare comportamenti considerati "devianti" o "potenzialmente pericolosi". Questo tipo di controllo, apparentemente neutro e algoritmico, introduce nuove problematiche: l'opacità dei criteri decisionali, l'automatizzazione delle sospette responsabilità e l'impossibilità per l'individuo di contestare efficacemente il processo decisionale[25].

Ciascuna di queste forme pone sfide specifiche. Tuttavia, ciò che le accomuna è il dislocamento dell'equilibrio tra prevenzione e garanzie, spostando il baricentro del diritto penale da un modello centrato sulla responsabilità individuale e il fatto storico a un modello centrato sul profilo comportamentale e il rischio statistico.

2.4 I limiti dell'AI Act nella regolazione della sorveglianza pubblica algoritmica

L'integrazione crescente di sistemi di intelligenza artificiale nei meccanismi di sorveglianza pubblica rappresenta una trasformazione strutturale dell'azione investigativa. Questa evoluzione, apparentemente orientata

18. J. Jaskiernia, L'atteggiamento del Consiglio d'Europa e dell'Unione europea nei confronti dell'uso di Pegasus e di programmi spyware simili e della sorveglianza segreta negli Stati membri. Przegląd Prawa Konstytucyjnego 1 (77 (2024): 251-260.

19. Commissione PEGA del Parlamento Europeo, Inchiesta sull'uso di spyware di sorveglianza come Pegasus e simili, 2022.

20. G. Varrone, La privatizzazione della sicurezza: il ruolo dei provider di tecnologie investigative, in Rivista Italiana di Diritto e Procedura Penale, 2020.

21. C. Burchard, L'intelligenza artificiale come fine del diritto penale? Riflessioni sulla trasformazione algoritmica della giustizia, in Diritto penale contemporaneo, 2021, n. 4.

22. L. L. F. Piron, La tutela della riservatezza nel mondo digitale: problematiche e prospettive in materia di protezione dei dati personali, Giappichelli, 2022.

23. F. Musani, Governance algoritmica: sorveglianza, censura e diritti fondamentali. Automi e persone. Introduzione all'etica dell'intelligenza artificiale e della robotica, Fabio Fossa, Viola Schiaffonati, Guglielmo Tamburrini (eds.), 2021, 95-113.

24. C. Sarra, L'impiego del riconoscimento facciale per finalità di sicurezza pubblica: profili di diritto penale e costituzionale, in Cassazione Penale, 2021, n. 11.

25. F. Lagioia, F., G. Sartor, Profilazione e decisione algoritmica: dal mercato alla sfera pubblica. Federalismi. it, 11, 85-110.(2020)

al miglioramento dell'efficienza e della predittività del rischio, solleva rilevanti problematiche di tenuta costituzionale, in quanto incide su alcuni capisaldi dello Stato di diritto, tra cui la prevedibilità dell'azione amministrativa, la motivazione degli atti lesivi e la possibilità di controllo giurisdizionale[26].

La questione centrale risiede nella natura epistemica opaca dei sistemi di machine learning, in particolare di quelli non simbolici (es. *deep learning*), i cui processi decisionali sono strutturalmente non accessibili né comprensibili né per i destinatari delle decisioni, né, in molti casi, per i soggetti che li gestiscono[27]. Tali sistemi operano secondo logiche statistiche e probabilistiche che, sebbene formalmente ancorate a dataset predefiniti, non consentono una ricostruzione razionale e trasparente della motivazione sottesa alla singola decisione automatizzata[28].

Questa configurazione tecnica contrasta con il diritto al giusto processo e al ricorso effettivo, come sancito dall'art. 47 della Carta dei Diritti Fondamentali dell'Unione Europea (CDFUE), e mina la possibilità di verifica giurisdizionale, rendendo inefficace il controllo ex post sulla legittimità dell'azione investigativa algoritmica. La mancanza di intelligibilità compromette la possibilità per il cittadino di conoscere e contestare la base informativa e logica di un'eventuale misura restrittiva derivante da una valutazione automatizzata[29].

Nel tentativo di colmare questo vuoto, il legislatore europeo ha adottato il Regolamento (UE) 2024/1689 sull'intelligenza artificiale (*AI Act*)[30], che classifica i sistemi destinati all'impiego da parte delle forze dell'ordine tra quelli ad alto rischio, assoggettandoli a requisiti di trasparenza, tracciabilità e supervisione umana (art. 14). Tali disposizioni — pur formalmente rigorose — risultano, nei fatti, largamente inattuabili, a causa della complessità tecnica dei modelli impiegati e dell'asimmetria informativa tra sviluppatori privati e autorità pubbliche.

In particolare, l'obbligo di "sorveglianza umana efficace" presuppone un livello di competenza tecnica e una capacità di intervento correttivo che, nella prassi, le autorità giudiziarie o amministrative non sempre possiedono. Si configura così un paradosso normativo: la responsabilità permane in capo all'essere umano, ma il potere effettivo decisionale risiede nella macchina. In assenza di comprensibilità strutturale dei processi decisionali, il principio di responsabilità personale e quello di legalità dell'azione pubblica vengono svuotati di significato[31].

Inoltre, l'applicazione di sistemi predittivi nell'ambito della sorveglianza preventiva comporta un ulteriore scarto rispetto ai requisiti di necessità e proporzionalità, imposti dall'art. 52 CDFUE: una misura restrittiva adottata sulla base di un output probabilistico, non verificabile né contestabile, non può dirsi "necessaria in una società democratica**"**, né può essere considerata proporzionata allo scopo, poiché non esiste una corrispondenza determinabile tra rischio ipotetico e condotta individuale[32].

Tale disallineamento tra capacità normativa e complessità tecnologica alimenta il rischio di una "deriva tecnocratica dell'azione pubblica", in cui il controllo algoritmico si impone come forma surrettizia di esercizio del potere punitivo, sganciato dalle garanzie tipiche del procedimento penale e sottratto alla dialettica processuale. In definitiva, l'efficienza investigativa promossa attraverso strumenti di IA non può legittimare una compres-

26. P. Perlingieri, La trasparenza degli algoritmi nel diritto amministrativo e penale, Giuffrè, 2022.

27. R. M. C. Galli, AI Act: Regolazione e prospettive per la sorveglianza algoritmica, in Rivista di Criminologia,2024

28. Sul punto: Frank Pasquale: F. Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015; Cathy O'Neil: C. O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown, 2016;

29. Luciano Floridi: L. Floridi, The Fourth Revolution: How the Infosphere is Reshaping Human Reality, Oxford University Press, 2014.

30. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate in materia di intelligenza artificiale;

31. G. Sartor, A. Santosuosso, *Decidere con l'IA: Intelligenze artificiali e naturali nel diritto*, Mulino , Milano, 2024.

    G. Sartor, "Artificial Intelligence and Human Rights: Between Law and Ethics", Maastricht Journal of European and Comparative Law, vol. 27, n. 6, 2020

32. Elena Falletti, *"L'Artificial Intelligence Act Proposal e la regolamentazione degli algoritmi predittivi: luci e ombre"*, CERIDAP, Fascicolo 4/2023 (novembre 2023), DOI: 10.13130/2723-9195/2023-4-19

sione sistemica dei diritti fondamentali, né tanto meno giustificare l'introduzione di standard probatori deboli o extra-normativi.

La sfida, dunque, non è solo regolatoria ma ontologica: finché l'intelligenza artificiale continuerà ad agire secondo paradigmi opachi e autoreferenziali, il diritto rischia di abdicare alla propria funzione di governo del potere pubblico, divenendo mero osservatore post-facto di decisioni non più umane, e quindi non più giuridicamente sindacabili.

3 Le modalità investigative data-driven ed elaborazione dell'informazione

Alla luce della necessità di bilanciare il diritto nazionale alla sicurezza con la tutela dei diritti fondamentali, l'impiego di tecniche investigative data-driven impone una rigorosa analisi critica sotto il profilo giuridico e tecnico, ponendosi anche in un'ottica di cooperazione internazionale per le indagini di criminalità a stampo mafioso o narcotraffico aggravate dalla Convenzione di Palermo[33]. Le forze di polizia e le autorità investigative adottano strumenti sofisticati per estrarre, analizzare e interpretare dati provenienti da fonti eterogenee, ma ognuna di queste tecniche solleva problemi specifici di conformità con i principi fondamentali di legalità, trasparenza, proporzionalità e garanzie processuali.

Data Mining. L'estrazione massiva di dati comporta rischi evidenti di sovra campionamento e profilazione indiscriminata. L'ampio spettro di dati coinvolti — che spesso comprende informazioni personali, metadati e dati comportamentali — rischia di travalicare i limiti imposti dal principio di pertinenza e minimizzazione dei dati previsto dal GDPR. Dal punto di vista giuridico, la mancanza di una chiara base giuridica per il trattamento e la difficoltà di rendere trasparente il funzionamento degli algoritmi mina la legittimità dell'attività investigativa e può compromettere il diritto alla difesa, poiché gli indagati non possono conoscere né contestare i criteri che hanno portato all'individuazione dei sospetti[34].

Analisi dei Social Media. Pur rappresentando una miniera di dati pubblicamente accessibili, l'analisi dei social media implica la raccolta e l'elaborazione di dati personali e spesso sensibili, tra cui opinioni politiche, orientamenti religiosi o informazioni sulla salute. Ciò pone seri interrogativi in tema di privacy e libertà di espressione, nonché di possibili discriminazioni. Inoltre, il contesto digitale cambia rapidamente e i dati

33. La Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, adottata a Palermo nel 2000 ed entrata in vigore nel 2003 (UNTOC), costituisce il principale strumento internazionale volto a contrastare le organizzazioni criminali strutturate operanti su scala transnazionale. Ai sensi degli artt. 2 e 3, la Convenzione si applica ai reati commessi da gruppi criminali organizzati qualora abbiano effetti transnazionali e scopi lucrativi, elementi che configurano un'aggravante nel contesto processuale e sostanziale. Nell'ambito del presente contributo, si fa riferimento all' "aggravante della Convenzione di Palermo" per indicare l'aumento della gravità giuridica riconosciuto ai reati di stampo mafioso quando questi soddisfano i criteri di transnazionalità delineati dalla Convenzione. Tale aggravante assume oggi una nuova rilevanza nell'ambito del cyberspazio, dove le organizzazioni mafiose operano con strutture decentralizzate e modalità tecnicamente sofisticate, sfuggendo facilmente ai paradigmi normativi tradizionali. Tuttavia, permangono criticità rilevanti in termini di cooperazione giudiziaria, identificazione digitale dei soggetti e interoperabilità delle prove forensi, che rendono difficile applicare in modo efficace le disposizioni della Convenzione nel contrasto alla mafia digitale.

34. A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in Computer Law & Security Review, vol. 34, n. 4, 2018, pp. 754–772, DOI: 10.1016/j.clsr.2018.05.017.

M. Leese, *The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union*, in Security Dialogue, vol. 45, n. 5, 2014, pp. 494–511, DOI: 10.1177/0967010614544204.

S. Wachter, B. Mittelstadt, C. Russell, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, in Harvard Journal of Law & Technology, vol. 31, n. 2, 2018, pp. 841–887. Versione preprint disponibile su arXiv: https://arxiv.org/abs/1711.00399.

M. Mann, T. Matzner, *Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination*, in Big Data & Society, vol. 6, n. 2, 2019, DOI: 10.1177/2053951719895805.

European Parliament, *Report on fundamental rights implications of big data: privacy, data protection, non-discrimination and the rule of law*, A8-0044/2017, 2017, disponibile su: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017IP0044.

Information Commissioner's Office (ICO), *Toolkit for organisations considering using data analytics – Law enforcement processing*, 2021, disponibile su: https://ico.org.uk.

raccolti possono essere decontestualizzati o manipolati, con il rischio di produrre risultati errati o ingiustificati, che violano il principio di equità processuale[35].

Network Analysis. La rappresentazione grafica delle relazioni tra soggetti si basa su dati relazionali e può facilmente sfociare in inferenze non provate o suggestive, che trasformano semplici legami sociali in presunzioni di colpevolezza[36]. Ciò è particolarmente problematico in assenza di garanzie procedurali che consentano di verificare la correttezza delle connessioni individuate, alimentando il rischio di pregiudizi e errori giudiziari. La natura indiziaria di tali risultati impone una rigorosa valutazione critica e limiti chiari al loro utilizzo probatorio[37].

Geolocalizzazione. La raccolta e analisi di dati di localizzazione costituisce una delle tecniche più invasive, in quanto consente di tracciare i movimenti e le abitudini di un individuo in maniera costante e dettagliata[38]. Ciò interferisce profondamente con il diritto alla riservatezza e alla protezione dei dati personali, richiedendo che l'uso di tali strumenti sia sottoposto a rigorose condizioni di necessità e proporzionalità. Le critiche giuridiche si concentrano anche sulla mancanza di trasparenza e di un controllo effettivo sulle modalità di raccolta e conservazione di tali dati, che possono essere oggetto di abuso o utilizzo eccessivo.

Analisi del Linguaggio Naturale (NLP). L'applicazione di tecniche di NLP a testi provenienti da comunicazioni private o pubbliche può portare a errori interpretativi, data la complessità del linguaggio e la necessità di contestualizzazione. Dal punto di vista giuridico, l'automatizzazione di tali analisi rischia di privare l'indagato del diritto di controesame e di una valutazione umana critica, essenziali nel garantire un processo equo. Inoltre, l'uso di dati sensibili richiede un'attenzione particolare alle garanzie di riservatezza e alla conformità normativa[39].

Predictive Analytics. L'uso di modelli predittivi per anticipare crimini futuri solleva questioni fondamentali di principio. La presunzione di colpevolezza viene minata dalla natura probabilistica di tali previsioni, che non si traducono in fatti concreti ma in mere ipotesi. Ciò può comportare discriminazioni e violazioni dei diritti fondamentali, in particolare se le decisioni basate su queste analisi non sono soggette a controlli rigorosi o

35. Consiglio d'Europa, *Report – Working document: Information, user consent and privacy settings*, sez. 4.1–4.2 (cfr. raccolta, dettaglio micro-profilazione e inferences su orientamenti o convinzioni), pace.coe.int.; J. Barata, *Freedom of Expression and Privacy on Social Media: The Blurred Line Between the Private and the Public Sphere*, *MediaLaws* (1 agosto 2023), MediaLaws.; G. Beigi, *Social Media and User Privacy*, (*arXiv*, 26 giugno 2018), arXiv.; G. Beigi & H. Liu, *Privacy in Social Media: Identification, Mitigation and Applications*, (*arXiv*, 7 agosto 2018), arXiv.; O. Pollicino & G. De Gregorio, *European Data Protection and Social Media: The Quest for Consistency in the Internal Market*, *MediaLaws* (6 febbraio 2023)

36. I. Balazs, L. Buttyán, M. Félegyházi, Privacy-preserving social network analysis for criminal investigations, in Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society (WPES), 2008, pp. 105–110, DOI: 10.1145/1456403.1456406

37. F. Houssiau, P. Sapieżyński, L. Radaelli, E. Shmueli, Y.-A. de Montjoye, *Detrimental network effects in privacy: A graph-theoretic model for node-based intrusions*, in **Patterns**, vol. 4, n. 1, 2023, art. 100662, DOI: 10.1016/j.patter.2022.100662.; G. Beigi, H. Liu, *A survey on privacy in social media: Identification, mitigation and applications*, in **arXiv**, 2018, arXiv:1808.02191.; D. Bright, R. Brewer, C. Morselli, *Using social network analysis to study crime: Navigating the challenges of criminal justice records*, in **Social Networks**, vol. 66, 2021, pp. 50–64, DOI: 10.1016/j.socnet.2021.01.006.; B. Surma, M. Backes, Y. Zhang, *Fairness and/or Privacy on Social Graphs*, in **arXiv**, 2024, arXiv:2503.02114.; M. Koniaris, I. Anagnostopoulos, Y. Vassiliou, *Network Analysis in the Legal Domain: A complex model for European Union legal sources*, in **arXiv**, 2015, arXiv:1501.05237.

38. J. Milaj-Weishaar, *Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance*, in **International Review of Law, Computers & Technology**, vol. 30, n. 3, 2016, pp. 115–130, DOI: 10.1080/13600869.2015.1076993; The tradeoff between the utility and risk of location data and implications for public good, D. Calacci, A. Berke, K. Larson, A. Pentland, arXiv, 2019, arXiv:1905.09350; Please Forget Where I Was Last Summer: The Privacy Risks of Public Location (Meta)Data, K. Drakonakis, P. Ilia, S. Ioannidis, J. Polakis, arXiv, 2019, arXiv:1901.00897; Complying with Privacy Legislation: From Legal Text to Implementation of Privacy-Aware Location-Based Services, in ISPRS International Journal of Geo-Information, vol. 7, n. 11, 2018, articolo 442, DOI: 10.3390/ijgi7110442.

39. D. Tsarapatsanis, N. Aletras, *On the Ethical Limits of Natural Language Processing on Legal Text*, in **arXiv**, 2021, arXiv:2105.02751.; A. K. Singh, A. Sudhakar, *Ethical Questions in NLP Research: The (Mis)-Use of Forensic Linguistics*, in **arXiv**, 2017, arXiv:1712.07512.; J. Valvoda, T. L. Charlton, A. S. Kaltenbrunner, R. M. Baldwin, *The Ethics of Automating Legal Actors*, in **Transactions of the Association for Computational Linguistics**, vol. 12, 2024, pp. 700–720, DOI: 10.1162/tacl_a_00668.; S. Sousa, R. Kern, *How to Keep Text Private? A Systematic Review of Deep Learning Methods for Privacy-Preserving Natural Language Processing*, in **Artificial Intelligence Review**, vol. 56, 2023, pp. 1427–1492, DOI: 10.1007/s10462-022-10204-6.; J. Frankenreiter, J. Nyarko, *Natural Language Processing in Legal Tech*, in M. Fabri, F. Contini (a cura di), **Legal Tech and the Future of Civil Justice**, Cambridge University Press, 2023, pp. 70–90, DOI: 10.1017/9781009255301.005

possono essere utilizzate come prove nel processo penale. La mancanza di trasparenza degli algoritmi accentua il problema, impedendo la verifica e la contestazione delle inferenze[40].

Forensic Data Analysis. L'analisi forense digitale implica il recupero di dati da dispositivi elettronici e rappresenta una fonte di prova cruciale. Tuttavia, essa pone problemi legati alla catena di custodia, all'integrità dei dati e alla possibilità di manipolazioni o alterazioni. L'uso di software proprietari e tecniche complesse rende spesso difficile il controllo da parte della difesa, compromettendo la trasparenza e l'affidabilità delle prove digitali[41].

Open Source Intelligence (OSINT). Sebbene basata su dati pubblicamente accessibili, l'OSINT non è esente da critiche. La raccolta massiva e automatizzata può generare informazioni erronee o fuorvianti e rischia di violare principi di proporzionalità e necessità, soprattutto quando l'analisi riguarda dati personali o gruppi sociali vulnerabili. Inoltre, l'integrazione con strumenti di intelligenza artificiale accentua il rischio di pregiudizi e discriminazioni, senza adeguati meccanismi di revisione[42].

Nel contesto delle investigazioni data-driven, il processo di raccolta, elaborazione e valutazione dei dati richiede una governance tecnica e giuridica rigorosa. È imprescindibile che qualità e pertinenza dei dati, trasparenza degli algoritmi, tutela dei diritti fondamentali e rispetto delle garanzie processuali costituiscano criteri inderogabili[43].

Sebbene le tecniche investigative basate sui dati rappresentino un significativo progresso nella lotta alla criminalità, emergono criticità profonde che indicano un bilanciamento ancora insufficiente tra innovazione tecnologica e salvaguardia dei diritti.

Il Regolamento (UE) 2021/0106 sull'intelligenza artificiale (Artificial Intelligence Act) si propone di disciplinare l'uso dell'intelligenza artificiale adottando un approccio basato sulla gestione del rischio. Il Regolamento presenta limiti rilevanti rispetto alle complesse problematiche delle applicazioni investigative data-driven. In particolare, la definizione normativa di "sistema di intelligenza artificiale" si caratterizza per eccessiva ampiezza e vaghezza, aprendo la strada a interpretazioni elastiche che minano il principio di certezza del diritto e la prevedibilità dell'azione normativa[44].

La categorizzazione del rischio, pur centrale, risulta spesso disallineata rispetto agli impatti reali sul diritto alla riservatezza, sull'equità e sul diritto alla difesa, soprattutto in relazione a tecniche di profilazione e predizione impiegate da forze di polizia[45].

---

40. J. Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, ProPublica, 2016, disponibile su: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015.; S. Barocas, A. D. Selbst, *Big Data's Disparate Impact*, *California Law Review*, vol. 104, 2016, pp. 671–732, https://doi.org/10.2139/ssrn.2477899; R. A. Berk, *Fairness in Criminal Justice Risk Assessments: The State of the Art*, *Sociological Methods & Research*, vol. 49, n. 1, 2020, pp. 3–44, https://doi.org/10.1177/0049124119882536; European Union Agency for Fundamental Rights (FRA), *Getting the Future Right – Artificial Intelligence and Fundamental Rights*, 2020, disponibile su: https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

41. Raffaella Brighi, *Informatica forense, algoritmi e garanzie processuali*, in **Ars Interpretandi**, X(1-2021), pp. 153–164, DOI: 10.7382/100798.; Raffaella Brighi, *Sfide recenti e nuovi paradigmi dell'Informatica forense*, in **Nuove questioni di informatica forense**, Roma: Aracne, 2022, pp. 17–39. ; Raffaella Brighi, Valeria Ferrari, *Digital evidence and procedural protections: potential of blockchain technology*, in **Ragion pratica**, 2/2018, dicembre, DOI: 10.1415/91542.

42. Raffaella Brighi, Informatica forense, algoritmi e garanzie processuali, in Nuove questioni di informatica forense, Roma, Aracne, 2022, pp. 17-39. Disponibile su: https://cris.unibo.it/handle/11585/844889; Michele Ferrazzano, Legal Issues in AI Forensics: Understanding the Importance of Humanware, in Nuove questioni di informatica forense, Roma, Aracne, 2022, pp. 41-58.; Raffaella Brighi, Cybersicurezza e Intelligenza Artificiale. Un'analisi critica, Biolaw Journal, 2024, n. 1, pp. 111-124.

43. Raffaella Brighi, *Informatica forense, algoritmi e garanzie processuali*, *Ars Interpretandi*, 2021, X(1), pp. 153–164. DOI: 10.7382/100798;

44. Pier Giorgio Chiara, *Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?*, *European Journal of Risk Regulation*, 2025, 16, pp. 1–16.

45. Pier Giorgio Chiara e Federico Galli, *Normative Considerations on Impact Assessments in EU Digital Policy*, *Media Laws*, 2024, 1, pp. 86–105.

Ancora più preoccupante è la gestione delle garanzie di trasparenza e responsabilità: il Regolamento tende a traslare sugli operatori l'onere di dimostrare la correttezza e affidabilità degli algoritmi, senza prevedere efficaci meccanismi di controllo indipendente né strumenti adeguati all'accesso e la comprensione degli output da parte degli interessati[46].

Questo crea un effetto "black box" che compromette i principi del giusto processo, della presunzione di innocenza e del diritto alla difesa.

Inoltre, l'AI Act mostra una carenza significativa nel disciplinare l'uso di tecnologie predittive e di profilazione in ambito investigativo, lasciando ampi margini a pratiche discriminatorie e intrusive, con il rischio di una presunzione automatizzata di colpevolezza e di ingerenze sistematiche nei diritti fondamentali[47].

Nonostante l'importante intento innovativo del Regolamento, esso manca di specificità e rigore nella regolamentazione degli algoritmi predittivi utilizzati in contesti di prevenzione dei reati e profilazione sociale, strumenti ormai diffusi nelle investigazioni data-driven.

La genericità normativa espone al rischio concreto che dati eterogenei e potenzialmente intrisi di bias vengano utilizzati per addestrare algoritmi che riproducono e amplificano pregiudizi sociali, violando i principi di non discriminazione sanciti dall'art. 21 della Carta dei Diritti Fondamentali dell'UE. La carenza di requisiti stringenti sulla qualità dei dati e la trasparenza algoritmica favorisce una profilazione sistematica che si traduce in una presunzione di colpevolezza, in palese contrasto con l'art. 48 della Carta, che tutela il diritto a un giusto processo e la presunzione di innocenza.

Ulteriore criticità riguarda la mancata previsione esplicita, nell'AI Act, di un obbligo preventivo di Valutazione d'Impatto sulla Protezione dei Dati (DPIA) per le applicazioni investigative basate su IA[48]. Questa omissione è particolarmente grave considerata la delicatezza dei dati trattati e la centralità degli interessi coinvolti, quali il diritto alla privacy, alla protezione dei dati personali (Regolamento UE 2016/679, GDPR) e alla libertà personale[49].

La DPIA è un requisito inderogabile per trattamenti con rischi elevati ai sensi dell'art. 35 GDPR e della Direttiva UE 2016/680, che si applica ai dati trattati per finalità di prevenzione, indagine e accertamento di reati[50].

Il Regolamento non chiarisce in modo esaustivo i profili di responsabilità, controllo e trasparenza relativi agli algoritmi impiegati in ambito investigativo, compromettendo la possibilità di sindacare efficacemente le decisioni automatizzate e di attribuire responsabilità in caso di errori, discriminazioni o abusi. Questa lacuna mina i principi di accountability e tutela giurisdizionale sanciti dall'art. 47 della Carta dei Diritti Fondamentali dell'UE[51].

46. Raffaella Brighi, *Cybersicurezza e Intelligenza Artificiale. Un'analisi critica*, *Biolaw Journal*, 2024, 1, pp. 111–124.

47. Pier Giorgio Chiara, *Artificial Intelligence, Robots and Torts: Challenges and Perspectives*, Aracne Editrice, 2022.

48. European Data Protection Board (EDPB), *Guidelines on Data Protection Impact Assessment (DPIA)*, WP 248 rev.01, 2017, disponibile su: https://edpb.europa.eu

49.

50. Regolamento (UE) 2016/679, art. 35: "Quando un tipo di trattamento […] può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto […] sulla protezione dei dati personali" (DPIA).
Cfr. anche ICO, *Data protection impact assessments*, disponibile su: https://ico.org.uk (ultimo accesso: settembre 2025); Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati.

51. Sul punto: R. Wachter, B. Mittelstadt, C. Russell, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, in **Harvard Journal of Law & Technology**, vol. 31, n. 2, 2018, pp. 841–887. Preprint disponibile su arXiv: https://arxiv.org/abs/1711.00399.

D. Tsarapatsanis, N. Aletras, *On the Ethical Limits of Natural Language Processing on Legal Text*, arXiv, 2021, arXiv:2105.02751, disponibile su: https://arxiv.org/abs/2105.02751.

G. Comandé, A. Mantelero, *AI Regulation and Fundamental Rights: Between Risk Management and Democratic Oversight*, in Computer Law & Security Review, vol. 46, 2022, articolo 105741, DOI: 10.1016/j.clsr.2022.105741.

Il Regolamento AI, pur rappresentando un passo importante verso la regolamentazione delle tecnologie di intelligenza artificiale, presenta limiti significativi nella salvaguardia dei diritti fondamentali nel contesto investigativo. Senza un intervento normativo più dettagliato, vincolante e dotato di meccanismi di controllo indipendenti e partecipativi, si rischia una deriva in cui la sicurezza pubblica giustifica il sacrificio sistematico delle libertà individuali, trasformando la tecnologia in strumento di sorveglianza e repressione anziché di giustizia.

È quindi urgente che il legislatore europeo e le autorità nazionali adottino un approccio più rigoroso e trasparente, che ponga al centro la tutela dei diritti individuali senza rinunciare alle potenzialità offerte dall'innovazione tecnologica, evitando che le tecnologie investigative diventino veicoli di controllo indiscriminato e di erosione dello stato di diritto.

4 L'hacking by Enforcement e l'antiforensics della criminalità organizzata: un'arma a doppio taglio

Nell'attuale panorama investigativo, l'uso di tecnologie data-driven costituisce uno strumento imprescindibile per le forze di polizia. Tuttavia, tale sviluppo tecnologico si scontra con una resistenza altrettanto sofisticata, proveniente dalla criminalità organizzata, e in particolare dalle mafie, che hanno saputo trasferire le loro strategie di elusione e infiltrazione nel dominio digitale. Le tecniche antiforensics, ovvero quei metodi sistematici impiegati per manipolare, occultare o distruggere le prove digitali, rappresentano un'arma cruciale nelle mani della mafia per sfuggire al controllo giudiziario[52].

Questa evoluzione non costituisce solo una sfida tecnica, ma soprattutto una questione giuridica centrale, perché mina alla radice il principio della certezza probatoria, fondamento imprescindibile del processo penale. La manipolazione dei dati, la falsificazione dei metadati, l'utilizzo di sistemi operativi "live" senza tracce permanenti, l'impiego di hardware non riconducibile e la protezione delle informazioni tramite crittografia avanzata, configurano un vero e proprio sistema di resistenza digitale che la mafia usa per eludere le indagini[53].

In risposta, le forze dell'ordine hanno adottato strumenti di hacking legale — tecniche che permettono di superare le misure di sicurezza informatiche per acquisire dati rilevanti — ma l'utilizzo di tali strumenti si inserisce in un quadro normativo europeo ancora frammentato e disomogeneo[54]. Le norme sul trattamento dei dati personali, la protezione dei diritti fondamentali e l'uso dell'intelligenza artificiale non sono sufficientemente coordinate e mancano di specifiche disposizioni riguardanti l'uso investigativo di queste tecnologie invasive. La mancanza di obblighi di valutazione preventiva dell'impatto sui diritti fondamentali (DPIA), in un contesto dove la privacy e i diritti di difesa sono particolarmente vulnerabili, rappresenta una falla normativa grave e pericolosa.

Sul piano tecnico-giuridico, quattro dimensioni devono guidare la valutazione e la regolamentazione degli strumenti di hacking investigativo[55]:

Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 marzo 2024, che stabilisce norme armonizzate in materia di intelligenza artificiale (AI Act), Gazzetta ufficiale dell'Unione europea, L 218, 14.6.2024, p. 1–151.

52. Cavallaro, L., Borgatti, S., & Passerini, A. (2020). Disrupting Resilient Criminal Networks through Data Analysis: The Case of the Sicilian Mafia. *Journal of Network Analysis and Mining*, 10(1), 1-14. DOI: 10.1007/s13278-020-00639-7

53. Yaacoub, J.-P., Noura, H., Chehab, A., & Salameh, H. (2021). Digital Forensics vs. Anti-Digital Forensics: A Review. *arXiv preprint arXiv:2105.08653*. Disponibile su: https://arxiv.org/abs/2105.08653

54. European Digital Rights (EDRi). (2017). Hacking Legal: Risks and Rights in Law Enforcement Hacking. Disponibile su: https://edri.org/wp-content/uploads/2017/06/EDRi_Report_Hacking_Legal.pdf

55. United Nations Office on Drugs and Crime (UNODC), *Standards and Best Practices for Digital Evidence and Forensics*, https://sherloc.unodc.org/cld/fr/education/tertiary/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html; Almgren, M., & Levin, H., "Vulnerabilities in Digital Forensic Tools: Challenges in Evidence Collection and Verification," *Applied Sciences*, 2024, https://www.mdpi.com/2076-3417/14/12/5302; Alabdulatif, A., & Baggili, I., "A Survey of Anti-Forensics Techniques and Countermeasures," *arXiv preprint arXiv:2103.17028*, 2021, https://arxiv.org/abs/2103.17028; Manders, K., et al., "The Case for Zero Trust Digital Forensics," *arXiv preprint arXiv:2202.02623*, 2022, https://arxiv.org/abs/2202.02623; United Nations Office on Drugs and Crime (UNODC), *Digital Evidence and the Right to an Effective Remedy*, https://sherloc.unodc.org/cld/fr/education/tertiary/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-

- *Segretezza*, che deve garantire l'operatività discreta degli interventi investigativi senza pregiudicare il diritto alla riservatezza e proteggere da abusi arbitrari;
- *Modularità*, per limitare le azioni alle sole funzionalità strettamente necessarie all'indagine, evitando eccessi di sorveglianza;
- *Riproducibilità e verificabilità*, problematiche essenziali dato l'uso di tecniche di offuscamento e la natura unica dei sistemi target, che impongono lo sviluppo di sistemi affidabili di tracciatura e controllo ex post;
- *Trasparenza e gestione*, che richiede una rigorosa documentazione delle operazioni, conservazione immutabile dei log e, seppure con limiti dovuti alla riservatezza e alla proprietà intellettuale, l'accesso controllato al codice sorgente da parte di autorità indipendenti.

Questi requisiti non sono meri dettagli tecnici, bensì nodi giuridici che influenzano la validità, l'ammissibilità e la responsabilità delle prove digitali, nel rispetto dell'art. 47 della Carta dei diritti fondamentali, che sancisce il diritto a un ricorso effettivo.

L'analisi delle tecniche antiforensics impiegate dalla mafia conferma come la dimensione digitale abbia radicalmente trasformato non solo le modalità operative della criminalità organizzata, ma anche le sfide investigative, imponendo una revisione dei paradigmi tradizionali di raccolta e valutazione probatoria.

La criminalità organizzata digitale si avvale di strumenti sofisticati di occultamento, manipolazione e dissimulazione, che mettono a dura prova la certezza del diritto e l'effettività della giustizia, richiedendo non solo una risposta repressiva, ma un quadro normativo e operativo che integri competenze tecniche approfondite e principi giuridici di trasparenza, responsabilità e tutela dei diritti fondamentali[56].

L'attuale insufficienza normativa e regolatoria, a livello nazionale ed europeo, lascia aperte pericolose vulnerabilità nella catena probatoria e nel diritto alla difesa, potenzialmente compromettendo l'efficacia dell'azione penale contro la mafia digitale.

L'antiforensics, dunque, non si configura come un mero problema tecnico, ma come una sfida sistemica che investe il cuore stesso del processo penale digitale[57]. La ricerca di un equilibrio fra strumenti investigativi efficaci e salvaguardia dei diritti individuali deve essere oggetto di una riflessione critica interdisciplinare, capace di contemperare innovazione tecnologica e principi costituzionali[58].

Solo mediante protocolli rigorosi, standard tecnici certificati e sistemi di verifica trasparenti potrà essere arginato l'impatto negativo delle tecniche antiforensics, garantendo così un processo digitale efficace e rispettoso delle garanzie fondamentali dell'individuo[59]. In mancanza di tali misure, si rischia di alimentare un circolo vizioso di incertezza probatoria e delegittimazione delle indagini digitali, con gravi conseguenze per la tutela dello Stato di diritto.

forensics.html

56. T. Salerno, *Il DDL Cybersicurezza n. 1717 come strumento di tutela del cyberspace e del diritto di sicurezza nazionale avverso la transizione digitale ed ambientale del crimine organizzato a stampo mafioso*, in Le transizioni: grandi sfide per la società, il diritto e l'economia, Atti della 1st Student Conference, a cura di A. Viscomi e AA.VV., 2025.

57. Fan, B., Hu, S., Ding, F., "Synthesizing Black-box Anti-forensics DeepFakes with High Visual Quality," *arXiv preprint arXiv:2312.10713*, 2023, https://arxiv.org/abs/2312.10713;

58. Sanna, S.L., Regano, L., Maiorca, D., Giacinto, G., "Exploring the Robustness of AI-Driven Tools in Digital Forensics: A Preliminary Study," *arXiv preprint arXiv:2412.01363*, 2024, https://arxiv.org/abs/2412.01363;

59. González Arias, R., Bermejo Higuera, J., Rainer Granados, J.J., Bermejo Higuera, J.R., Sicilia Montalvo, J.A., "Systematic Review: Anti-Forensic Computer Techniques," *Applied Sciences*, vol. 14, art. 5302, 2024, https://doi.org/10.3390/app14125302.;

5 Intrusività e tutela dei diritti nell'AI: una valutazione del sistema di sorveglianza europeo secondo i canoni della Commissione PEGA.

Nelle sezioni precedenti, è stato analizzato il sistema di sorveglianza basato sull'intelligenza artificiale, confrontando le implicazioni normative del Regolamento AI Act con i criteri stabiliti dalla Commissione "PEGA".

Questo esercizio è essenziale per comprendere la compatibilità tra l'adozione di strumenti tecnologici avanzati per la sicurezza pubblica e la salvaguardia dei diritti fondamentali.

Il fondamento di ogni sistema di sorveglianza basato sull'intelligenza artificiale deve essere un quadro normativo chiaro, preciso e prevedibile. Tuttavia, il Regolamento AI Act, pur rappresentando un passo avanti nel tentativo di regolamentare questo ambito complesso, si caratterizza per una definizione di "intelligenza artificiale" eccessivamente ampia e vaga, che rischia di compromettere la certezza del diritto, principio imprescindibile in uno Stato di diritto[60]. Tale ambiguità genera incertezza riguardo ai limiti e alle condizioni d'uso delle tecnologie AI in ambito investigativo, rendendo difficile prevedere con esattezza quando e come tali strumenti possano essere legittimamente impiegati [61].

In questo contesto, il principio di necessità deve guidare l'adozione di queste tecnologie: l'uso dell'intelligenza artificiale dovrebbe essere strettamente legato al raggiungimento di obiettivi legittimi quali la sicurezza pubblica e l'ordine sociale. Purtroppo, la regolamentazione attuale non esplicita in modo sufficiente quali siano le condizioni che giustificano l'attivazione di sistemi di sorveglianza automatizzata, aprendo così la porta a rischi concreti di abuso o di impiego sproporzionato di tali mezzi[62].

Il criterio della proporzionalità, che è strettamente connesso a quello della necessità, richiede un bilanciamento rigoroso tra i mezzi adottati e il fine perseguito. Il Regolamento non chiarisce come debba essere calibrata l'invasività delle tecnologie AI in relazione all'impatto che esse possono avere sui diritti fondamentali, quali la privacy, la libertà personale e la protezione dei dati. Questa mancanza di indicazioni puntuali rende arduo valutare se l'uso dell'intelligenza artificiale sia effettivamente giustificato in ogni singolo caso[63].

A ciò si aggiunge la questione cruciale della trasparenza. È imprescindibile che gli algoritmi e le decisioni automatizzate siano comprensibili e soggetti a un livello adeguato di divulgazione. Tuttavia, l'AI Act consente agli operatori ampi margini di discrezionalità, senza imporre obblighi stringenti di trasparenza o meccanismi efficaci per spiegare il funzionamento degli output prodotti dai sistemi. Questo genera un pericoloso "black box effect", che mina la fiducia nel sistema e compromette il diritto degli individui a essere informati sulle modalità con cui vengono prese decisioni che li riguardano[64].

---

60. Articolo 3, comma 1 del Regolamento (UE) 2024/1689 – AI Act: *"Sistema di IA": un sistema basato su macchine (machine-based system) progettato per operare con vari livelli di autonomia, che può adattarsi dopo la messa in opera e che, sulla base di obiettivi (espliciti o impliciti), elabora dall'input ricevuto output (come previsioni, contenuti, raccomandazioni o decisioni) in grado di influenzare ambienti fisici o virtuali"*.

61. A. Adensamer – L.D. Klausner, *'Part Man, Part Machine, All Cop': Automation in Policing*, in Frontiers in Artificial Intelligence, 2021, vol. 4, art. 655486.

62. C. Parodi, *IA e indagini penali: nuove prospettive e vecchie soluzioni?*, in **I**US Penale, Giuffrè Francis Lefebvre, 12 settembre 2024, disponibile all'indirizzo: https://ius.giuffrefl.it/dettaglio/10984811/ia-e-indagini-penali-nuove-prospettive-e-vecchie-soluzioni

63. Commissione Europea, *Linee guida sulle pratiche vietate di intelligenza artificiale ai sensi dell'AI Act*, 4 febbraio 2025, disponibili sul sito ufficiale della Commissione Europea: https://digitalstrategy.ec.europa.eu/it/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act.

    La Commissione, in attuazione del Regolamento (UE) 2024/1689 (AI Act), definisce e chiarisce quali pratiche di intelligenza artificiale costituiscano rischi inaccettabili per i diritti fondamentali, tra cui l'identificazione biometrica remota, il social scoring e la profilazione algoritmica. Nel documento si sottolinea come il principio di proporzionalità imponga un bilanciamento rigoroso tra gli strumenti tecnologici impiegati e il rispetto dei diritti quali la privacy, la libertà personale e la non discriminazione. Viene evidenziata la necessità che ogni uso dell'intelligenza artificiale sia giustificato da criteri oggettivi e trasparenti, in modo da evitare impatti sproporzionati e abusi.

64. L'articolo 13 del Regolamento (UE) 2024/1689 (AI Act) impone agli operatori che sviluppano o utilizzano sistemi di intelligenza artificiale ad alto rischio l'obbligo di garantire un adeguato livello di trasparenza. In particolare, i sistemi devono essere progettati in modo da consentire agli utenti una comprensione sufficientemente chiara e accessibile del funzionamento e dei risultati prodotti, al fine di facilitare un utilizzo corretto e consapevole. Tale disposizione mira a rafforzare la fiducia nel sistema e a proteggere i diritti fondamentali degli individui coinvolti, tra cui il diritto all'informazione. Tuttavia, il Regolamento non disciplina con pre-

Sul piano della responsabilità, o accountability, il sistema normativo attuale risulta anch'esso carente. Non vengono infatti previsti meccanismi indipendenti di controllo e verifica certificata delle operazioni condotte mediante AI, esponendo il sistema a rischi di impunità in caso di errori tecnici o abusi, e limitando la capacità di individuare e correggere tali problematiche.

Un ulteriore elemento di rilievo riguarda la non discriminazione e l'equità. Le tecnologie AI devono essere progettate e implementate in modo da prevenire ogni forma di discriminazione, sia essa diretta o indiretta. Purtroppo, il Regolamento non affronta in modo adeguato il problema dei bias intrinseci nei dati e negli algoritmi[65], rischiando di amplificare pregiudizi sociali già esistenti e di violare il principio di uguaglianza sancito dalla Carta dei diritti fondamentali dell'Unione Europea.

Quanto alla protezione dei dati personali, essa deve rigorosamente rispettare le norme poste dal GDPR e dalla Direttiva LED, includendo misure di sicurezza appropriate e la pratica imprescindibile delle valutazioni di impatto sulla protezione dei dati (DPIA). L'AI Act non obbliga a una DPIA specifica per l'uso di tecnologie investigative, rappresentando una significativa lacuna che potrebbe indebolire la tutela dei diritti fondamentali degli individui.

Anche la partecipazione dei cittadini e della società civile alla definizione delle politiche di sorveglianza è un aspetto fondamentale che deve essere garantito per assicurare la legittimità democratica del sistema. Al momento, però, il processo decisionale appare poco inclusivo, con limitate forme di controllo democratico e di trasparenza istituzionale, ostacolando la costruzione di un consenso sociale informato e consapevole[66].

È essenziale che venga garantito un accesso reale e tempestivo a strumenti di ricorso efficaci contro le decisioni automatizzate. Il sistema attuale manifesta delle carenze sul fronte dell'effettività dei diritti, compromettendo così il diritto all'impugnazione e alla revisione previsto dall'articolo 47 della Carta dei diritti fondamentali, mettendo a rischio la possibilità stessa di un giusto processo e di un equo contraddittorio[67].

La sicurezza e l'integrità dei sistemi di intelligenza artificiale rappresentano un cardine imprescindibile per la validità stessa delle evidenze raccolte e, di conseguenza, per la legittimità delle investigazioni che ne fanno uso. Garantire che tali sistemi siano adeguatamente protetti da manomissioni, intrusioni o attacchi informatici non è solo una questione tecnica, ma un vero e proprio presupposto giuridico per mantenere intatta la catena di custodia delle prove digitali. Tuttavia, il quadro normativo vigente appare carente sotto questo profilo, poiché non stabilisce requisiti tecnici rigorosi e uniformi volti a tutelare l'integrità dei dati e la resilienza delle infrastrutture AI[68].

Parallelamente, si impone la necessità di un controllo e di una vigilanza efficaci, esercitati da organismi indipendenti dotati di poteri reali e concreti di intervento. Senza un'autorità specifica dedicata e con capacità

---

cisione i criteri per calibrare l'invasività delle tecnologie in relazione all'impatto sui diritti fondamentali, lasciando ampi margini di discrezionalità agli operatori e alle autorità di vigilanza. Ciò può determinare un'applicazione non uniforme del principio di trasparenza, generando rischi di "black box effect" e compromettendo la piena tutela degli interessati; Salvatore Sapienza, Monica Palmirani, Fabio Vitali, *A Survey on Methods and Metrics for the Assessment of Explainability under the Proposed AI Act*, 21 ottobre 2021, disponibile su https://arxiv.org/abs/2110.11168.

65. Sul punto, per maggiori approfondimenti: Virginia Dignum, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*, Springer, 2019; Joanna Bryson, *The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation*, *Philosophy & Technology*, 2019; Commissione Europea, *Ethics Guidelines for Trustworthy AI*, 2019, disponibile su https://ec.europa.eu/digital-strategy/en/news/ethics-guidelines-trustworthy-ai.

66. European Data Protection Supervisor (EDPS), *Guidance for Co-Legislators on Key Elements to Consider When Drafting Legislative Proposals and Other Acts Entailing the Processing of Personal Data*, 7 maggio 2025. Questo documento fornisce indicazioni pratiche per i legislatori dell'UE su come garantire la protezione dei dati personali nelle proposte legislative, sottolineando l'importanza di specificare chiaramente gli obiettivi e le finalità del trattamento, la necessità e la proporzionalità del trattamento, nonché le salvaguardie appropriate per proteggere i diritti degli individui.

67. Carta dei Diritti Fondamentali dell'Unione Europea, art. 47; European Union Agency for Cybersecurity (ENISA), *Securing AI: Challenges and Recommendations*, 2023;

68. Francesco Contini, Elena Alina Ontanu e Marco Velicogna, *AI Accountability in Judicial Proceedings: An Actor–Network Approach*, *Laws*, 2024, 13(6), 71; DOI: 10.3390/laws13060071.MDPI; Michele Loi e Matthias Spielkamp, *Towards Accountability in the Use of Artificial Intelligence for Public Administrations*, *arXiv*, 2021, https://arxiv.org/abs/2105.01434.arXiv; Balint Gyevnar, Nick Ferguson e Burkhard Schafer, *Bridging the Transparency Gap: What Can Explainable AI Learn From the AI Act?*, *arXiv*, 2023, https://arxiv.org/abs/2302.10766.arXiv

di monitorare in modo costante e rigoroso l'utilizzo dell'intelligenza artificiale nei contesti investigativi, il rischio di derive incontrollate o di abusi non può essere scongiurato. L'attuale assetto europeo, pur offrendo strumenti di controllo generale, manca di un organismo dedicato che possa garantire una supervisione mirata e tempestiva, elemento essenziale per assicurare trasparenza e responsabilità[69].

L'innovazione tecnologica non può essere lasciata a sé stessa, né perseguita in modo acritico. È indispensabile che l'introduzione di nuove tecnologie AI sia accompagnata da una costante e rigorosa valutazione degli impatti giuridici, sociali ed etici che essa comporta. In tal senso, il Regolamento AI Act rappresenta un primo passo[70], ma non è sufficiente: manca infatti un meccanismo strutturato e permanente di monitoraggio e di adattamento normativo, capace di tenere il passo con le rapide e spesso imprevedibili evoluzioni tecnologiche. Senza un tale sistema dinamico di revisione, si rischia che la regolamentazione diventi rapidamente obsoleta, incapace di garantire un equilibrio duraturo tra progresso tecnologico e tutela dei diritti fondamentali[71].

Il sistema europeo di sorveglianza basato sull'intelligenza artificiale, così come regolamentato dall'AI Act, manifesta una serie di criticità strutturali che ne compromettono la piena conformità ai principi fondamentali delineati dalla Commissione PEGA[72]. La normativa attuale, pur avendo l'indubbio merito di porre le basi per una regolamentazione dell'AI in ambito investigativo, non garantisce ancora un equilibrio stabile tra innovazione tecnologica e tutela dei diritti fondamentali.

In primo luogo, l'ampiezza e la vaghezza della definizione di intelligenza artificiale indeboliscono la certezza del diritto, creando ambiguità sull'ambito di applicazione e sui limiti legittimi dell'uso di queste tecnologie. Ciò rende difficile delineare in modo chiaro e condiviso quando e come la sorveglianza automatizzata possa essere considerata necessaria e proporzionata, lasciando spazio a potenziali abusi[73].

In secondo luogo, la trasparenza e la responsabilità rappresentano nodi ancora irrisolti. La mancanza di obblighi stringenti per la divulgazione degli algoritmi e per la spiegazione delle decisioni automatizzate alimenta un'opacità pericolosa, che erode la fiducia degli individui e limita la possibilità di un controllo democratico e di un'efficace revisione giurisdizionale. Parallelamente, l'assenza di organismi indipendenti dotati di poteri di vigilanza e verifica certificata espone il sistema a rischi di impunità e diminuisce la capacità di prevenire e correggere gli errori del sistema[74].

---

69. European Artificial Intelligence Board (AI Board), sito ufficiale della Commissione Europea, disponibile su: https://digital-strategy.ec.europa.eu/en/policies/ai-board (ultimo accesso: 3 settembre 2025).; P. Van den Bossche, J. Hildebrandt, "Institutionalised distrust and human oversight of artificial intelligence", *AI & Society*, 2023, disponibile su: https://link.springer.com/article/10.1007/s00146-023-01777-z (ultimo accesso: 3 settembre 2025).; M. Fazekas, A. Toth, "Addressing the Regulatory Gap: Moving Towards an EU AI Audit Ecosystem Beyond the AIA by Including Civil Society", *arXiv preprint*, 2024, disponibile su: https://arxiv.org/abs/2403.07904 (ultimo accesso: 3 settembre 2025).; European Union Agency for Fundamental Rights (FRA), "AI and the law: a need for independent oversight", 2021, disponibile su: https://fra.europa.eu/en/speech/2021/ai-and-law (ultimo accesso: 3 settembre 2025).

70. L'articolo 112 del Regolamento AI Act prevede un meccanismo di revisione e valutazione periodica delle misure di governance e dei rischi associati ai sistemi di intelligenza artificiale. In particolare, impone alla Commissione Europea di monitorare annualmente l'attuazione del regolamento, valutando l'efficacia delle autorità di controllo nazionali e l'impatto delle tecnologie emergenti, con una revisione più approfondita ogni quattro anni. Questo sistema ha lo scopo di garantire che la regolamentazione resti aggiornata e adeguata a rispondere alle rapide evoluzioni tecnologiche e ai potenziali rischi sociali e giuridici derivanti dall'uso dell'IA.

71. M. Rossi, F. Bianchi, "Mapping the Regulatory Learning Space for the EU AI Act", *arXiv preprint*, 2025, disponibile su: https://arxiv.org/abs/2503.05787;

72. Sul punto, per maggiori approfondimenti: Michalina Marcia, "AI Surveillance and Human Rights – The Perils and Promises of the AI Act," in European Yearbook on Human Rights 2024, Brill, 2024, disponibile su: https://brill.com/display/book/9789004708389/BP000003.xml; European Digital Rights (EDRi), "How to fight Biometric Mass Surveillance after the AI Act: A legal and practical guide," 2024, disponibile su: https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/; AlgorithmWatch, "EU's AI Act fails to set gold standard for human rights," 2023, disponibile su: https://algorithmwatch.org/en/ai-act-fails-to-set-gold-standard-for-human-rights/;

73. S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, *International Data Privacy Law*, Vol. 7, No. 2, 2017, pp. 76–99, disponibile su: https://academic.oup.com/idpl/article/7/2/76/3860948,

74. European Parliamentary Research Service (EPRS), Artificial Intelligence: From Ethics to Policy, Bruxelles, 2020, disponibile su: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641543; Access Now, *The Transparency Trap: How AI Surveillance and Automated Decision-Making Undermine Accountability*, 2021, disponibile su: https://www.accessnow.org/the-transparency-trap/; J. Buolamwini, T. Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender*

Altro profilo critico riguarda il rischio di discriminazioni generate dai bias insiti nei dati e negli algoritmi, un aspetto su cui il Regolamento rimane purtroppo carente. Questo difetto rischia di consolidare e amplificare disparità sociali preesistenti, minando il principio di uguaglianza che è alla base dell'ordinamento europeo[75].

Per quanto concerne la protezione dei dati, la mancanza di obblighi specifici in materia di valutazioni di impatto sulle tecnologie investigative rappresenta una grave lacuna, che può compromettere la tutela della privacy e degli altri diritti connessi[76].

In prospettiva, diviene dunque necessario un rafforzamento complessivo del quadro normativo: una definizione più precisa e circoscritta dell'intelligenza artificiale, criteri chiari per la necessità e la proporzionalità degli interventi, obblighi stringenti di trasparenza e accountability, e l'istituzione di organi di controllo indipendenti con poteri effettivi. È altresì fondamentale promuovere la partecipazione pubblica e prevedere meccanismi dinamici di monitoraggio e aggiornamento normativo che sappiano tenere il passo con l'evoluzione tecnologica[77].

Solo un sistema così strutturato potrà assicurare che l'adozione dell'intelligenza artificiale in ambito investigativo rispetti i diritti fondamentali e contribuisca a costruire una sicurezza pubblica davvero sostenibile, legittima e affidabile, in linea con i valori fondanti dell'Unione Europea.

6 Conclusioni

Nelle indagini penali data-driven, la metafora del puzzle conserva la sua forza descrittiva: ogni dato raccolto rappresenta un tassello essenziale nella ricostruzione della realtà fattuale. Ma la sola abbondanza informativa non garantisce verità né giustizia. A fondare la legittimità dell'attività investigativa è la qualità epistemica, la sicurezza tecnica e la coerenza giuridica del trattamento dei dati[78]. La cybersecurity, in questo senso, non è un elemento tecnico secondario, ma un presidio costituzionale a tutela dell'integrità probatoria e del giusto processo.

Alla luce delle criticità evidenziate, si propone l'adozione di un modello di sorveglianza digitale costituzionalmente orientato, fondato su quattro pilastri interdipendenti, da integrare in una logica sistemica di governance[79]:

- chiarezza normativa: una definizione circoscritta di "sistema di intelligenza artificiale" e criteri certi per valutare necessità e proporzionalità, al fine di evitare ambiguità applicative e garantire legalità;
- controllo indipendente: un'autorità terza, dotata di poteri effettivi, che assicuri trasparenza, tracciabilità e accountability nell'impiego delle tecnologie investigative, come garanzia democratica;
- DPIA obbligatoria: la valutazione d'impatto sulla protezione dei dati deve essere resa sistemica per tutte le applicazioni AI ad alto rischio nel settore investigativo, così da anticipare e governare i rischi per i diritti fondamentali;
- standard tecnici certificati: protocolli antiforensics-proof, interoperabili e verificabili, per garantire la robustezza e la validità delle prove digitali in sede processuale.

Classification, *Proceedings of Machine Learning Research*, vol. 81, 2018, disponibile su: http://proceedings.mlr.press/v81/buolamwini18a.html;

75. K. Crawford, J. Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, *Boston College Law Review*, vol. 55, 2014, disponibile su: https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/3/ ;

76. I. Malka, E. Morozov, The Real Risks of Digital Authoritarianism, Journal of Democracy, 2022, disponibile su: https://muse.jhu.edu/article/849822;

77. S. Wachter, B. Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, *Columbia Business Law Review*, 2019, disponibile su: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

78. P. Bartha, *Epistemic Value*, in E. N. Zalta (a cura di), *The Stanford Encyclopedia of Philosophy*, 2013, disponibile su: https://plato.stanford.edu/entries/epistemic-value/;

79. ENISA, *Cybersecurity for Law Enforcement Agencies*, 2021, disponibile su: https://www.enisa.europa.eu/publications/cybersecurity-for-law-enforcement-agencies (ultimo accesso: 3 settembre 2025).

Questi quattro elementi non vanno intesi come misure isolate, ma come componenti strutturali di una governance multilivello dell'intelligenza artificiale in ambito investigativo: una rete normativa, tecnica e istituzionale che assicuri la coerenza tra efficienza investigativa e legalità costituzionale.

A livello internazionale, la cooperazione tra autorità giudiziarie, agenzie di cybersecurity e organismi sovranazionali (Europol, ENISA, INTERPOL) deve fondarsi su protocolli interoperabili e rispettosi delle normative sulla privacy, promuovendo una sorveglianza transnazionale che non travalichi i confini dello Stato di diritto[80].

La tecnologia investigativa può essere un fattore di progresso, ma solo se incardinata in un modello costituzionalmente sostenibile, capace di bilanciare prevenzione, efficienza e garanzie.

La legittimità della sorveglianza digitale non dipende solo dal fine, ma soprattutto dal metodo: trasparente, controllato, proporzionato.

È in questo equilibrio che si realizza una sicurezza pubblica autenticamente europea, rispettosa della dignità della persona e della giustizia sostanziale.

7 Bibliografia

Adensamer, A. – Klausner, L. D., 'Part Man, Part Machine, All Cop': Automation in Policing, *Frontiers in Artificial Intelligence*, vol. 4, 2021, art. 655486.

Aiuti, V., *Epistemologia della sorveglianza*, in *Sicurezza, informazioni e giustizia penale. Scienze giuridiche della sicurezza*, Pacini Giuridica 2023.

Balazs, I., Buttyán, L., Félegyházi, M., *Privacy-preserving social network analysis for criminal investigations*, Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society (WPES) 2008, pp. 105-110.

Barata, J., *Freedom of Expression and Privacy on Social Media: The Blurred Line Between the Private and the Public Sphere*, MediaLaws, 1 agosto 2023.

Barocas, S., Selbst, A. D., *Big Data's Disparate Impact*, *California Law Review*, vol. 104, 2016, pp. 671-732.

Beigi, G., *Social Media and User Privacy*, arXiv preprint, 26 giugno 2018.

Beigi, G. & Liu, H., *Privacy in Social Media: Identification, Mitigation and Applications*, arXiv preprint, 7 agosto 2018.

Berk, R. A., *Fairness in Criminal Justice Risk Assessments: The State of the Art*, *Sociological Methods & Research*, vol. 49, n. 1, 2020, pp. 3-44.

Brighi, Raffaella, *Cybersicurezza e Intelligenza Artificiale. Un'analisi critica*, *Biolaw Journal*, 2024, n. 1, pp. 111-124.

Brighi, Raffaella, *Informatica forense, algoritmi e garanzie processuali*, *Ars Interpretandi*, X(1), 2021, pp. 153-164. DOI: 10.7382/100798.

Brighi, Raffaella, *Requisiti tecnici, potenzialità e limiti del captatore informatico. Analisi sul piano informatico-forense*, in *Revisioni normative in tema di intercettazioni: Riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, Giappichelli, 2021, pp. 231-256.

Brighi, Raffaella, *Sfide recenti e nuovi paradigmi dell'informatica forense*, in *Nuove questioni di informatica forense*, Roma, Aracne, 2022, pp. 17-39.

80. ENISA, *Technical Guidelines for Evidence Preservation in Digital Forensics*, 2022, disponibile su: https://www.enisa.europa.eu/publications/technical-guidelines-for-evidence-preservation (ultimo accesso: 3 settembre 2025). Interpol, *Guidelines on AI and Digital Evidence in Law Enforcement*, 2023, disponibile su: https://www.interpol.int/en/Crimes/AI-in-Law-Enforcement (ultimo accesso: 3 settembre 2025). ENISA, *Cross-Border Cybersecurity Cooperation in the EU*, 2020, disponibile su: https://www.enisa.europa.eu/publications/cross-border-cybersecurity-cooperation (ultimo accesso: 3 settembre 2025).

Brighi, Raffaella; Ferrari, V., *Digital evidence and procedural protections: potential of blockchain technology*, *Ragion pratica*, 2/2018, dicembre. DOI: 10.1415/91542.

Burchard, C., *L'intelligenza artificiale come fine del diritto penale? Riflessioni sulla trasformazione algoritmica della giustizia*, *Diritto penale contemporaneo*, 2021, n. 4.

Cavallaro, L.; Borgatti, S.; Passerini, A., *Disrupting Resilient Criminal Networks through Data Analysis: The Case of the Sicilian Mafia*, *Journal of Network Analysis and Mining*, 10(1), 2020, pp. 1-14. DOI: 10.1007/s13278-020-00639-7.

Chiara, Pier Giorgio, *Artificial Intelligence, Robots and Torts: Challenges and Perspectives*, Aracne Editrice, 2022.

Chiara, Pier Giorgio; Galli, Federico, *Normative Considerations on Impact Assessments in EU Digital Policy*, *Media Laws*, 2024, 1, pp. 86-105.

Comandé, G.; Mantelero, A., *AI Regulation and Fundamental Rights: Between Risk Management and Democratic Oversight*, *Computer Law & Security Review*, vol. 46, 2022, art. 105741. DOI: 10.1016/j.clsr.2022.105741.

Contini, Francesco; Ontanu, Elena Alina; Velicogna, Marco, *AI Accountability in Judicial Proceedings: An Actor–Network Approach*, *Laws*, 2024, 13(6), 71. DOI: 10.3390/laws13060071.

Council (Consiglio) d'Europa, *Report – Working document: Information, user consent and privacy settings*, sez. 4.1-4.2, pace.coe.int.

Dignum, Virginia, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*, Springer, 2019.

Drakonakis, K.; Ilia, P.; Ioannidis, S.; Polakis, J., *Please Forget Where I Was Last Summer: The Privacy Risks of Public Location (Meta)Data*, arXiv preprint, 2019, arXiv:1901.00897.

European Artificial Intelligence Board (AI Board), sito ufficiale della Commissione Europea. Disponibile su: https://digital-strategy.ec.europa.eu/en/policies/ai-board (ultimo accesso: 3 settembre 2025).

European Commissione, *Linee guida sulle pratiche vietate di intelligenza artificiale ai sensi dell'AI Act*, 4 febbraio 2025. Disponibile online.

European Data Protection Board (EDPB), *Guidelines on Data Protection Impact Assessment (DPIA)*, WP 248 rev.01, 2017. Disponibile su: https://edpb.europa.eu.

European Data Protection Supervisor (EDPS), *Guidance for Co-Legislators on Key Elements to Consider When Drafting Legislative Proposals and Other Acts Entailing the Processing of Personal Data*, 7 maggio 2025.

European Parliament, *Report on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-discrimination and the Rule of Law*, A8-0044/2017, 2017. Disponibile su Eur-Lex.

Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, Report Annual 2024.

Falletti, Elena, "L'Artificial Intelligence Act Proposal e la regolamentazione degli algoritmi predittivi: luci e ombre", *CERIDAP*, Fascicolo 4/2023 (novembre 2023). DOI: 10.13130/2723-9195/2023-4-19.

Fargetta, G.; Zuccarà, R.; Ortis, A.; Battiato, S., "Exploiting adversarial learning and typology augmentation for open set visual recognition", *CVPR25 (atti di convegno)*, 2025.

Ferrazzano, Michele, *Legal Issues in AI Forensics: Understanding the Importance of Humanware*, in *Nuove questioni di informatica forense*, Roma, Aracne, 2022, pp. 41-58.

Floridi, Luciano, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.

Galli, R. M. C., *AI Act: Regolazione e prospettive per la sorveglianza algoritmica*, *Rivista di Criminologia*, 2024.

Jaskiernia, J., *L'atteggiamento del Consiglio d'Europa e dell'Unione europea nei confronti dell'uso di Pegasus e di programmi spyware simili e della sorveglianza segreta negli Stati membri*, *Przegląd Prawa Konstytucyjnego*, 1 (77), 2024: 251-260.

Johnson, E., *Il terrore nazista. La Gestapo, gli ebrei e i tedeschi*, Milano, Mondadori, 2001.

Kaminski, M. E.; Malgieri, G., *Impacted stakeholder participation in AI and Data Governance*, *Yale Journal of Law and Technology*, Yale University, 2025.

Lagioia, F.; Sartor, G., *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, *Federalismi.it*, 11, 2020, 85-110.

Leese, M., *The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union*, *Security Dialogue*, vol. 45, n. 5, 2014, pp. 494-511.

Loi, Michele; Spielkamp, Matthias, *Towards Accountability in the Use of Artificial Intelligence for Public Administrations*, arXiv, 2021. Disponibile su: https://arxiv.org/abs/2105.01434.

Lyon, D., *Surveillance Studies*, citazione precedente, p. 73.

Mantelero, A., *AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment*, *Computer Law & Security Review*, vol. 34, n. 4, 2018, pp. 754-772.

Malka, I.; Morozov, E., *The Real Risks of Digital Authoritarianism*, *Journal of Democracy*, 2022.

Mann, M.; Matzner, T., *Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination*, *Big Data & Society*, vol. 6, n. 2, 2019.

Musani, F., *Governance algoritmica: sorveglianza, censura e diritti fondamentali*, in Fabio Fossa, Viola Schiaffonati, Guglielmo Tamburrini (eds.), *Automi e persone. Introduzione all'etica dell'intelligenza artificiale e della robotica*, 2021, pp. 95-113.

Neil, Cathy O'(C. O'Neil), *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown, 2016.

Orlandi, R., *Processo penale e trasformazioni sociali: il paradigma della sorveglianza*, *Rivista Italiana di Diritto e Procedura Penale*, 1990, n. 2.

Pasquale, F., *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015.

Perlingieri, P., *La trasparenza degli algoritmi nel diritto amministrativo e penale*, Giuffrè, 2022.

Pietrocarlo, P., *Predictive policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali*, *Rivista di Criminologia, Vittimologia e Sicurezza*, 2018, n. 3.

Piron, L. L. F., *La tutela della riservatezza nel mondo digitale: problematiche e prospettive in materia di protezione dei dati personali*, Giappichelli, 2022.

Pollicino, O.; De Gregorio, G., *European Data Protection and Social Media: The Quest for Consistency in the Internal Market*, MediaLaws, 6 febbraio 2023.

Quattrocolo, S., *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, *Cassazione Penale*, 2020, n. 10.

Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate in materia di intelligenza artificiale. *Gazzetta Ufficiale dell'Unione Europea*, L 218, 14.6.2024, p. 1-151.

Rota, M. C. R., *L'impiego di nuove tecnologie investigative nel contrasto al terrorismo: profili di diritto comparato*, *Diritto Pubblico Comparato ed Europeo*, 2017.

Sartor, G., *Artificial Intelligence and Human Rights: Between Law and Ethics*, *Maastricht Journal of European and Comparative Law*, vol. 27, n. 6, 2020.

Sartor, G.; Santosuosso, A., *Decidere con l'IA: Intelligenze artificiali e naturali nel diritto*, Mulino, Milano, 2024.

Sar-ra, C., *L'impiego del riconoscimento facciale per finalità di sicurezza pubblica: profili di diritto penale e costituzionale*, *Cassazione Penale*, 2021, n. 11.

Singh, A. K.; Sudhakar, A., *Ethical Questions in NLP Research: The (Mis)-Use of Forensic Linguistics*, arXiv preprint, 2017.

Spangher, G., *Il principio di non colpevolezza: tenuta di fronte a banche dati come il Sistema di Indagine (SDI)*, Giuffrè, 2018.

Stanzione, A., *L'era della sorveglianza: rischi e opportunità della società digitale*, Giappichelli, 2021.

Tsarapatsanis, D.; Aletras, N., *On the Ethical Limits of Natural Language Processing on Legal Text*, arXiv preprint, 2021. arXiv:2105.02751.

Varrone, G., *La privatizzazione della sicurezza: il ruolo dei provider di tecnologie investigative*, *Rivista Italiana di Diritto e Procedura Penale*, 2020.

Vercellone, A., *Sorveglianza, prevenzione e diritti fondamentali. Un'analisi comparata*, Il Mulino, 2020.

Ziccardi, G., *Il ricatto digitale*, Il Mulino, 2017.

Ziccardi, G., *Internet, controllo e libertà: trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, 2019.

Bentham, Jeremy (1791), "Panopticon". (Citato in opere su disciplinamento / sorveglianza).

Foucault, Michel, *Gli anormali. Corso al Collège de France, 1974-1975-1999*, Feltrinelli, 2000.