Journal of Ethics and Legal Technologies – Volume 8(1) – April 2026

La *predictive policing* vista dalla prospettiva dei *surveillance studies*. Un'analisi attraverso i concetti di sorveglianza e *dataveillance*

Leonardo Marchesin

Università degli Studi di Padova

Abstract: Today, predictive policing is undergoing a period of considerable geographical expansion, and its technical evolution is experiencing a season of remarkable growth thanks to the continuous development of algorithmic systems. In scientific literature, predictive policing operations and their consequences are often examined from a procedural perspective, but they also involve a series of processes and elements which occupy a central position in a different, albeit related, scientific field, that is the field of surveillance studies. For this reason, the aim of this paper is to propose an analysis of predictive policing using some conceptual tools specific to surveillance studies. To do so, it seemed appropriate to draw on two central concepts in this field: dataveillance, coined in 1988 by Roger Clarke, and surveillance, which dates back to modern times and is now embodied above all by the phenomenon of video-surveillance. This analysis revealed the composite nature of predictive policing. In fact, it consists of two main phases. The first one involves the collection and storage of data and can therefore be framed within the conceptual boundaries of dataveillance. The second phase involves monitoring by law enforcement agencies of individuals and social groups identified through data: here, we can see the typical features of traditional surveillance. The link between these two phases is an essential moment of algorithmic analysis. The usefulness of adopting an approach based on surveillance studies can thus be twofold. On the one hand, it allows to grasp in a linear manner the typical features of the functioning of predictive policing mechanisms, i.e., a unitary phenomenon resulting from the harmonious intertwining of several distinct phases. On the other hand, the perspective of surveillance studies allows to bear in mind that each of the phases of predictive policing encompasses issues of significance for both the individual and society. In the context of predictive policing, these critical issues do not seem to cancel each other out or mitigate each other. On the contrary, they persist and tend to intertwine, sometimes ending up reinforcing each other. An example of this danger can be seen in the possibility of a "targeted" chilling effect, i.e. an effect typical of surveillance mechanisms that is intended to be produced on individuals and social groups previously identified through dataveillance tools.

Keywords: predictive policing, surveillance, dataveillance, chilling effect.

1. Sorveglianza, videosorveglianza e *dataveillance* nei *surveillance studies*

Provare a tracciare i confini di un ambito scientifico quale quello dei *surveillance studies* rappresenta senz'altro un'impresa ardua. Da un lato, infatti, essi costituiscono, per usare le parole di David Lyon, una «cross-disciplinary enterprise», ovverosia una disciplina destinata ad interessare numerosi settori del sapere umano, da ciascuno dei quali, peraltro, è possibile appropinquarvisi attraverso categorie concettuali e strumenti scientifici di volta in volta differenti e tra loro complementari[1]. Dall'altro lato, Gary T. Marx ha evidenziato opportunamente la consistenza anche storica degli studi sulla sorveglianza, i quali «came to increased public and academic attention after the events of 9/11», pur avendo destato «interest to scholars at least since the 1950s»[2]. Entro un contesto tanto variegato nelle sue diverse prospettive di ricerca, quanto caratterizzato da uno sviluppo cronologico tutt'altro che circoscritto, il principale, se non unico, elemento comune e trasversale pare essere rappresentato dallo stesso oggetto di indagine al centro dei *surveillance studies*, ovverosia il fatto che, ancora secondo Lyon, «for whatever reason, people and populations are under scrutiny»[3].

La condizione di essere *under scrutiny* che è fulcro degli studi sulla sorveglianza e che, tanto in contesti comuni quanto negli studi specialistici, viene meglio indicata con il termine, appunto, *sorveglianza*, costituisce a propria volta un concetto di difficile definizione, benché ad esso vi si ricorra con frequenza. Tale nozione, infatti, rinvia a pratiche sociali assai risalenti nel tempo, pur avendo trovato una più compiuta teorizzazione soltanto in età moderna, epoca a partire dalla quale, peraltro, essa, lungi dal trovare una definitiva cristallizzazione, ha sperimentato numerosi mutamenti e ripensamenti, tutt'ora in atto[4].

Una pur rapida ricostruzione etimologica potrebbe aiutare a meglio inquadrare il nucleo di un concetto tanto complesso. La parola *sorvegliare* deriva dal vocabolo francese *sur-veiller*, che, letteralmente, significa vegliare (*-veiller*) su (*-sur*) qualcuno o qualcosa, e che, a propria volta, discende dal verbo latino *vigilare*, in uso per indicare l'azione compiuta da colui che è desto,

[1] Lyon, 2002, 5. Lyon propone un elenco molto vasto di settori scientifici interessati dai *surveillance studies*, tra i quali vengono ricordati la sociologia, le scienze politiche, la geografia, la storia e la filosofia, l'informatica e le scienze dell'informazione, il diritto, la psicologia sociale e l'antropologia, la letteratura, la filmologia e una lunga serie di altri studi incentrati su fenomeni come globalizzazione, lavoro, media e consumismo: cfr. *ibidem*.

[2] Marx, 2015, 735.

[3] Lyon, 2002, 2.

[4] Per una ricognizione delle varie fasi storiche vissute dal fenomeno della sorveglianza cfr. Surace, 2005.

sveglio, attento, e che, più nello specifico, sta adempiendo mansioni di guardia e custodia. Come è stato evidenziato da Gary T. Marx, una simile radice etimologica indurrebbe a identificare l'essenza della sorveglianza, quantomeno con riferimento all'ambito umano, nel «regard or attendance to others (whether a person, a group, or an aggregate as with a national census) or to factors presumed to be associated with these»[5], perlopiù attraverso l'utilizzo dello sguardo. Il prefisso *sur-*, inoltre, sembrerebbe attribuire addirittura una direzionalità a tale attività di focalizzazione dell'attenzione, la quale seguirebbe un moto *dall'alto verso il basso*, da un'entità sovra-ordinata (es. lo Stato) ad una sotto-ordinata (es. il suddito/cittadino)[6].

Giova, peraltro, ricordare che, al momento della sua prima enucleazione in età moderna, tale attività di osservazione si accompagnava, quasi intrinsecamente, ad una condizione di visibilità dell'osservatore agli occhi dell'osservato. David Lyon ha ricordato, infatti, che, benché la figura del guardiano fosse diffusa già presso le civiltà antiche, la sorveglianza fu «professionalised as a "policing" task in eighteenth century Europe», quando, nel 1829, «Robert Peel established the Metropolitan Police in London, [...] one of their roles was to *be visible* in "preventive patrolling"»[7].

Dunque, dall'unione della sua radice etimologica e delle principali pratiche che, in epoca moderna, contribuirono a consolidarne per la prima volta il significato, risulta che la sorveglianza, intesa quantomeno nel suo nucleo primordiale, si configura come un'attività di focalizzazione dell'attenzione (soprattutto visiva) sull'essere umano, da parte di un'entità ad esso sovra-or-

[5] Marx, 2015, 734. Nel panorama della letteratura scientifica in materia, tale nozione generalissima sembra costituire il solo e minimo comune denominatore rispetto ad una congerie di definizioni non sempre collimanti e tra loro coerenti. David Lyon identifica la sorveglianza con «the focused, systematic and routine *attention* to personal details» (corsivo aggiunto), e in essa rinviene un naturale anelito a perseguire «the purposes of influence, management, protection or direction»: Lyon, 2007, 14. Secondo uno schema non del tutto sovrapponibile, e dopo aver ricordato che «etimologicamente *sorveglianza* deriva dal vocabolo francese *surveiller*», e che, quindi, significa «letteralmente *vigilare su* qualcosa o qualcuno», Michela Michetti individua il fine intrinseco di tale azione nell'«attingere informazioni, dati o elementi, predittivi ed utili per conoscere tendenze, caratteristiche, opinioni e comportamenti sia individuali che collettivi»: Michetti, 2023, 547.

[6] Questo profilo appare evidente se si considera la genesi del neologismo *sousveillance*, impiegato da Jean-Gabriel Ganascia: «the word sousveillance is a neologism built on the model of 'surveillance', the latter from French *sur*, meaning 'over' and *veiller*, 'to watch', and which literally means 'watching from above'. By analogy, sousveillance has been built to designate the act of watching (*veiller*) from below (*sous*). In the case of sousveillance, the *watchers* are socially below those who are watched, while in the case of surveillance it is the opposite, they are above»: Ganascia, 2010, 5.

[7] Lyon, 2022, 6. Lyon riconosce, tuttavia, che in alcuni ambiti – quali quello militare – pattugliamento e sorveglianza sono pratiche esercitate sin da epoca moderna ricorrendo al nascondimento dell'osservatore agli occhi dell'osservato: cfr. *ibidem*.

dinata, attuata anche attraverso una (parziale) esposizione del sorvegliante al sorvegliato.

Come anzidetto, negli ultimi due secoli le pratiche di sorveglianza hanno subito numerose alterazioni quantitative e altrettante variazioni qualitative, connesse tanto a rilevanti mutamenti politici, sociali ed economici, quanto, soprattutto, a sviluppi tecnologici via via sempre più rapidi e sostanziali. Ed è proprio entro tale flusso evolutivo che, nel maggio 1988, è emersa la nozione di *dataveglianza*. Come noto, tale neologismo è stato coniato da Roger Clarke allo scopo di definire «the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons»[8]. In altri termini, con la nozione di *dataveglianza* si andrebbe ad indicare una pratica di focalizzazione dell'attenzione non più sulla persona fisica, bensì sulla congerie di dati e metadati che, nell'universo digitale, concorrono a comporne il corpo virtuale[9]. Tale attività, resa possibile dalla generazione e dalla disponibilità di ingenti quantità di informazioni, da plurime tecnologie tanto potenti quanto diffuse, nonché da immensi *dataset* tra loro fluidamente interconnessi[10], è esercitata in forme decentralizzate[11] e sembra escludere qualsivoglia possibilità di reciprocità tra un sorvegliato sempre più trasparente[12] ed un sorvegliante sempre più invisibile[13].

Con la *dataveglianza*, dunque, pare configurarsi uno scarto notevole e sostanziale rispetto al paradigma tradizionale di sorveglianza, e non solo in ragione dei dispositivi tecnologici che hanno progressivamente reso possibile e continuano tutt'oggi a consentire simili nuove forme di monitoraggio. Queste ultime, infatti, si configurano, globalmente, come una pratica che preferisce captare dati e metadati relativi all'essere umano anziché osservarlo direttamente, che assume una dimensione ubiquitaria e decentralizzata che "orizzontalizza" – seppur non completamente - un rapporto in passato

[8] Clarke, 1988, 499.

[9] Cfr. Perri, 2020, 27, e Maestri, 2015, 84. Sul concetto di corpo virtuale/elettronico cfr. Rodotà, 2018, 73 ss.

[10] Cfr. Michetti, 2023, 564. Secondo Pierluigi Perri, addirittura, «ciò che distingue la *dataveglianza* rispetto alle altre forme di sorveglianza sinora illustrate sono proprio i mezzi tecnologici mediante i quali essa viene esercitata», in quanto «non ci sarebbe mai potuta essere una *dataveglianza* senza la potenza di calcolo e la velocità delle reti telematiche che conosciamo ora, perché la mole di dati che ne riesce ad esprimere il potenziale necessita di un apparato tecnologico molto avanzato»: Perri, 2020, 25.

[11] Cfr. Maestri, 2015, 84.

[12] Pierluigi Perri ricorda che la *dataveglianza* può essere rivolta «verso uno specifico individuo (*dataveglianza* individuale) ma anche verso un gruppo più o meno vasto di persone (*dataveglianza* di massa)»: Perri, 2020, 24.

[13] Cfr. Fioriglio, 2015, 15. Sulla generale inconsapevolezza dell'individuo medio della quantità di dati che produce quotidianamente e della sorveglianza che li riguarda cfr., tra i molti, Ziccardi, 2022, *passim*; Zuboff, 2019, 288-289; Focarelli, 2015, 9-10.

fortemente gerarchico o comunque verticale, e che tende a nascondere del tutto il sorvegliante ad un sorvegliato sempre più inconsapevole di essere tale.

Tuttavia, l'avvento della *dataveillance* non pare aver eliminato completamente forme di monitoraggio che, per quanto fondate oggi sull'impiego di sistemi e meccanismi ben più all'avanguardia rispetto a quelli utilizzati nei secoli passati, sembrano realizzare, ancora nel tempo presente, il significato primigenio della sorveglianza. Tale è il caso della videosorveglianza. Come noto, con questa denominazione si è soliti indicare ciò che, già nel 2005, Stefano Rodotà definiva «una moda»[14], ovverosia quella di collocare un ingente numero di telecamere all'interno dei tessuti urbani. Le videocamere integrano la nozione originaria di sorveglianza assai più della *dataveglianza* identificata da Clarke. Innanzitutto, esse puntano i propri occhi elettronici direttamente sugli individui e non sulle loro informazioni, osservando corpi e comportamenti in quanto tali e non in qualità di privilegiate fonti di dati. In secondo luogo, a servirsi della videosorveglianza nei confronti dei cittadini sono ancora entità che rispetto ad essi godono generalmente di una posizione sovra-ordinata, derivante, se non già dalla loro natura pubblica o statuale, quantomeno dal fatto di vantare la titolarità di un maggior numero di prerogative all'interno del contesto di riferimento (si pensi all'impianto di videosorveglianza installato dal commerciante all'interno del proprio negozio)[15]. Inoltre, come ha evidenziato Adam Greenfield, le telecamere «sono fatte apposta per essere viste»[16] da coloro che si intende sorvegliare, oltre che per vederli a propria volta[17]. Da ultimo, si potrebbe anche osservare come, a differenza della *dataveillance*, le videocamere siano ancora chiamate ad assolvere principalmente – ma non solo – una funzione di tutela, deterrenza e sicurezza assai simile a quella svolta dalla Metropolitan Police di Londra a partire dal XIX secolo[18]. In altri termini, la videosorveglianza si presenta come una riproposizione della moderna sorveglianza in chiave tecnologicamente evoluta e al passo con i tempi, capace di sostituire il limitato occhio umano con quello implacabile di un dispositivo elettronico.

Nell'attuale società sorvegliata, pertanto, sembrano coesistere due diverse forme di "veglianza": una più vicina alla nozione tradizionale e primigenia di

[14] Rodotà, 2005, 71. Rispetto al contesto cinese, Josh Chin e Liza Lin hanno più di recente osservato che «la proliferazione delle telecamere […] aveva reso l'atto di guardare e di essere guardati un gesto normale della vita»: Chin e Lin, 2022, 220-221.

[15] Si pensi, ad esempio, all'ingente numero di videocamere installate a Londra da enti pubblici a fini di sicurezza, registrazione dell'affluenza e gestione della circolazione stradale: cfr. Tulumello, 2013, 33-34.

[16] Greenfield, 2017, 50.

[17] Si pensi all'esempio emblematico delle *dummy cameras*: cfr. Fonio, 2006, 270.

[18] Cfr. Fonio, 2009, 103, e Fonio, 2007, 132.

sorveglianza (la videosorveglianza), e una che, invece, se ne discosta quanto a oggetto e modalità del monitoraggio, nonché con riguardo alla posizione del sorvegliante rispetto al sorvegliato (la *dataveglianza*). Ciò non significa certo che queste due dinamiche di monitoraggio rappresentino due realtà tra loro nettamente scisse. Esse, al contrario, si configurano come fenomeni tra loro interconnessi, tanto a livello teorico quanto sul piano pratico. Ed è proprio questa relazione che si intende indagare attraverso il presente contributo, assumendo, in particolar modo, la prospettiva privilegiata fornita da un universo in costante evoluzione, ovverosia quello della polizia predittiva (o *predictive policing*), oggi al centro di un vivace dibattito interno ed internazionale che, tuttavia, è più avvezzo a sottolinearne i profili processuali che quelli che la ricollegano ai *surveillance studies*.

Si procederà, anzitutto, effettuando una ricognizione del fenomeno della polizia predittiva, al fine di comprendere quali caratteri essa condivida con le due forme di "veglianza" qui individuate, nonché quale particolare relazione queste ultime instaurino tra loro al suo interno. Successivamente, si ritornerà sulle dinamiche della videosorveglianza e della *dataveglianza* per esaminarne, separatamente, le rispettive implicazioni negative, tanto per i singoli individui quanto per le comunità che essi concorrono a costituire. Tale disamina sarà essenziale per mostrare come simili effetti pregiudizievoli rischino di mescolarsi e rafforzarsi a vicenda proprio all'interno delle pratiche di *predictive policing*, con ciò fornendo ulteriore sostegno all'idea di una vera e propria interoperabilità tra le due forme di "veglianza" ora presentate. Tale percorso permetterà non solo di meglio comprendere il funzionamento e i caratteri della polizia predittiva attraverso una sua disamina condotta utilizzando le categorie generali di (video)sorveglianza e *dataveillance*, ma anche di osservare, per il tramite di una pratica concreta quale è quella della *predictive policing*, come queste due realtà si relazionino tra loro, e come una simile interazione possa condurre ad un potenziamento dei pericoli da esse rispettivamente derivanti.

2. La *predictive policing* tra sorveglianza e *dataveillance*

Parlare di polizia predittiva significa occuparsi di un fenomeno di estrema attualità e rilevanza, ma che rappresenta pur sempre un tassello di un puzzle ben più ampio. Mauro Santaniello, infatti, ha ricordato che quello della *predictive policing* è «solo uno dei tanti campi di applicazione della valutazione algoritmica», intendendosi con quest'ultima espressione «un processo che non si limita ad assegnare punteggi sulla base di una sommatoria di valori predefiniti pur ponderati, ma che produce previsioni e decisioni sulla base di un sistema di indicatori doppiamente dinamico perché, da un lato, si nutre

costantemente di nuovi dati raccolti dalle fonti più disparate d'informazione ed elaborati in un processo iterativo virtualmente senza fine, e dall'altro si modifica autonomamente grazie alle proprie capacità autoriflessive e di apprendimento»[19].

Tale collocazione rende evidente come lo sviluppo del fenomeno noto come polizia predittiva debba considerarsi relativamente recente, in quanto inscindibilmente connesso alla progettazione degli innovativi strumenti di raccolta di ingenti quantità di dati, nonché degli algoritmi necessari ad elaborarli[20]. Tuttavia, per quanto innovativa, la *predictive policing* non sembra implicare lo svolgimento, da parte delle forze dell'ordine, di attività completamente nuove rispetto a quelle passate: come ha notato Beatrice Perego, infatti, per molti aspetti essa si presenta, piuttosto, «come una replica del lavoro precedentemente riservato ai soli operatori umani»[21]. In altri termini, attraverso la polizia predittiva, a mutare non sarebbe tanto la tipologia delle operazioni di polizia, quanto piuttosto i mezzi tecnici con i quali esse vengono condotte, e le cui potenzialità hanno comunque condotto ad alcune alterazioni quantitative e qualitative di rilievo affatto secondario.

Muovendo dal piano temporale a quello spaziale, è necessario notare come quello della *predictive policing* rappresenti un fenomeno geograficamente esteso, diffusosi ben oltre i confini statunitensi che ne accolsero le prime sperimentazioni[22]. Benché, infatti, l'impiego della polizia predittiva assuma un carattere sistematico perlopiù in alcune delle maggiori metropoli degli Stati Uniti (Los Angeles, New York, Santa Cruz, etc.), esso risulta oramai frequente anche in Europa, come evidenziato, ad esempio, da Simon Egbert con riguardo alla realtà tedesca[23] e da Angelica Bonfanti in relazione alla realtà danese[24].

L'appartenenza ad un contesto socio-tecnologico ampio e variegato, la tensiva posizione di medietà tra attività tradizionali di polizia e utilizzo di strumenti in costante evoluzione, e la diffusione presso città e Nazioni tra loro assai differenti per storia, cultura ed ordinamento giuridico rendono

[19] Santaniello, 2019, 86 e 99.

[20] Cfr. Ferguson, 2019, 492. Si vedano i tentativi di raccolta dati e previsione algoritmica da parte della polizia di New York (cfr. Willis, Mastrofski e Weisburd, 2007) e della California (cfr. Bratton e Malinowski, 2008). Sulle origini della polizia predittiva cfr. Ferguson, 2017b, 29 ss.

[21] Perego, 2020, 449. Anche Andrew Ferguson ha ritenuto che «the short history of predictive policing begins with the long history of criminology. The idea that crime patterns can be studied, mapped, and analyzed has deep roots. Place-based criminology can be traced back to the mid-1800s with researchers studying particular areas of localized crime»: Ferguson, 2019, 492.

[22] Cfr. Santaniello, 2019, 92, e Velo Dalbrenta, 2017, 54.

[23] Cfr. Egbert, 2018.

[24] Cfr. Bonfanti, 2018, 207-208.

tutt'altro che agevole il compito di individuare una nozione univoca e onnicomprensiva di *predictive policing*. Nella letteratura scientifica di riferimento, numerosi sono stati e continuano ad essere i tentativi di addivenire ad una definizione completa di polizia predittiva. Tra le molte, una delle più richiamate e stimate è quella offerta da Walter L. Perry *et al.*, secondo il quale «predictive policing is the application of analytical techniques - particularly quantitative techniques - to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions»[25].

Tale nozione di polizia predittiva presenta l'indubbio vantaggio di porre l'attenzione della dottrina su quella che è la principale promessa lanciata dal fenomeno qui in esame, ovverosia quella di permettere non solo di *solve past crimes* ma soprattutto di *prevent crime*. È senz'altro vero ciò che ha affermato Andrew Ferguson, ovverosia che «predictive policing technology is not one thing that can be categorized, but involves different approaches, technologies, and theories»[26]. Tuttavia, l'assunto di base che funge inevitabilmente da premessa logica a qualsiasi tentativo di polizia predittiva – indipendentemente dai costrutti teorici e pratici che concretamente lo animano - è dato dalla convinzione che il crimine possa essere non solo represso ma anche previsto[27], e che, dunque, sia possibile - prima ancora che utile - adottare verso di esso un approccio proattivo anziché esclusivamente reattivo[28]. In altre parole, la *predictive policing* viene utilizzata nella convinzione che essa possa anzitutto prevedere e prevenire i reati, così da essere impiegata al fine di ridurre il tasso di criminalità entro un determinato contesto di riferimento[29].

L'obiettivo principale della polizia predittiva viene perseguito attraverso una serie di procedure tese ad innalzare il grado di oggettività ed accuratezza delle operazioni di polizia[30], così da rendere possibile un'allocazione delle risorse a disposizione delle forze dell'ordine che garantisca una maggiore efficienza nella loro gestione e una migliore efficacia delle prestazioni tramite esse erogate[31]. Riassumere brevemente il funzionamento di codesti sistemi, tra loro differenti e risultanti dall'interpolazione di procedimentalità algoritmica e attività umana, non è impresa facile, ma Lucio Camaldo sembra

[25] Perry *et al.*, 2013, xiii.

[26] Ferguson, 2019, 493. Ferguson ha individuato, in particolare, tre nuclei teorici principali, tutti tesi alla previsione e alla prevenzione della criminalità, ma sulla base di assunti differenti: la *Hot Spot Policing*, la *Problem-Oriented Policing* e la *Community-Oriented Policing*: cfr. *ivi*, 498-503.

[27] Cfr. Di Nicola *et al.*, 2014, 7.

[28] Cfr. Camaldo, 2025, 63; Pietrocarlo, 2024, 4-5; Pietrocarlo, 2023, 2; Mugari e Obioha, 2021, 1; Benbouzid, 2019, 1; Ferguson, 2017a, 1137; Velo Dalbrenta, 2017, 53-54.

[29] Cfr. Pietrocarlo, 2023, *passim*.

[30] Cfr. Pietrocarlo, 2024, 4, e Perego, 2020, 464.

[31] Cfr. Basile, 2022, 5; Meijer e Wessels, 2019, 1033-1034; Velo Dalbrenta, 2017, 54.

avere correttamente individuato le «tre fasi» di cui qualsiasi procedimento di *predictive policing* necessita di valersi per assolvere le proprie funzioni: «la prima consiste nell'inserimento dei dati (di una o più tipologie) nel sistema; segue, poi, l'analisi dei dati inseriti attraverso un metodo algoritmico, allo scopo di elaborare la specifica previsione cui il sistema è finalizzato; infine, tale previsione viene utilizzata da parte degli operatori di polizia per adottare le decisioni strategiche e le tattiche sul campo»[32].

Tuttavia, contenuto e svolgimento dei tre step appena menzionati subiscono variazioni affatto irrilevanti a seconda della categoria generale nella quale rientrano i sistemi di polizia predittiva di volta in volta presi in considerazione. Come noto, essi possono essere divisi, in ragione dei loro obiettivi specifici, in (almeno) due categorie, ovverosia i *place-based systems* e i *person-based systems*[33]. Le principali divergenze tra questi due modelli, già intuibili dalle loro rispettive denominazioni, sono state di recente esplicitate con chiarezza da Elisabetta Pietrocarlo. I sistemi *place-based* «rappresentano i sistemi più risalenti ma tuttora maggiormente diffusi», e «mirano a individuare le aree geografiche nelle quali, in un determinato arco temporale, è altamente probabile siano commessi reati, cosicché gli agenti possano intensificare i controlli con l'obiettivo di prevenire l'attività criminale ovvero di arrestare in flagranza i relativi autori»[34]. Viceversa, i sistemi *person-based* «sono diretti all'identificazione dei potenziali autori o vittime di reati»[35], e tra essi è possibile identificare un sotto-gruppo, quello dei *suspect-based systems*, i quali, «analizzando i dati relativi a precedenti reati di carattere seriale (come, ad esempio, le rapine), tentano di cogliere alcuni tratti comuni a elaborare il profilo – anonimo – del possibile autore»[36], e ciò per assolvere, a seconda delle esigenze, una funzione repressiva ovvero preventiva.

Come è possibile comprendere già da queste definizioni, le differenze contenutistiche delle previsioni attese nei diversi modelli di *predictive policing* determinano anzitutto una disparità nelle tipologie di dati da raccogliere e successivamente inserire quali *input* nell'analisi algoritmica. Seguendo ancora una volta le parole di Lucio Camaldo, appare chiaro che, mentre i *place-based systems* necessitano soprattutto di «dati e informazioni sugli eventi criminali», con particolare attenzione «alla distribuzione geografica del crimine e al ritmo delle attività giornaliere», i *person-based systems* «richiedono la compilazione di elenchi di persone ritenute "a rischio", nonché una *social*

[32] Camaldo, 2025, 63.
[33] Su tale categorizzazione cfr. *ibidem*; Pietrocarlo, 2024, 5; Basile, 2022, 7-8; Algeri, 2021, 729; Polidoro, 2020, 6-7.
[34] Pietrocarlo, 2024, 5. Cfr. anche Lonati, 2022, 309; Perego, 2022, 450; Ferguson, 2017b, 63.
[35] Pietrocarlo, 2024, 7. Cfr. anche Hung e Yen, 2021, 165 ss., e Meijer e Wessels, 2019, 1034.
[36] Pietrocarlo, 2024, 9.

network analysis»[37], per effettuare le quali si rendono necessari dati dalla foggia inevitabilmente diversa. Se, dunque, è vero che inserendo all'interno del sistema algoritmico alcuni *input* invece di altri si ottengono *output* correlativamente diversi, deve altrettanto ammettersi che al fine di ottenere una determinata previsione (una mappa degli *hot spots* o un elenco di persone sospette) sarà necessario raccogliere alcuni specifici dati (geografici o personali) e non altri.

Ma anche sul versante delle tattiche concrete adottate sulla base degli *output* risultati dall'elaborazione algoritmica possono intervenire alcune variazioni, a seconda che il sistema utilizzato sia *place-based* o *person-based*. Nel caso dei primi, la strategia generalmente adottata sembra alquanto omogenea, ed è stata efficacemente spiegata da Andrew Ferguson: «once identified, the forecast area is targeted for more police deterrence», il che significa che «police officers make their presence known in an effort to deter criminals»[38]. Relativamente ai secondi, invece, l'attività successiva alla predizione algoritmica risulta essere più articolata, in quanto connessa allo svolgimento e agli esiti di un eventuale futuro giudizio penale. Come ha spiegato Elisabetta Pietrocarlo, essa generalmente si sostanzia «nell'invito ad astenersi dal commettere ulteriori reati, pena la possibilità di incorrere in conseguenze di rilievo, tra cui l'irrogazione di una sanzione più severa in ragione del precedente avvertimento»[39].

A fronte della panoramica che ne è stata ora offerta, è possibile osservare la polizia predittiva attraverso le due speciali lenti offerte dagli altrettanti modelli teorici di monitoraggio individuati nel paragrafo precedente, ovverosia la sorveglianza e la *dataveglianza*.

Anzitutto, si è visto che, indipendentemente dalla loro natura e dal loro contenuto, i dati rappresentano il punto di partenza essenziale delle attività di *predictive policing*, le quali non possono che prendere avvio proprio dalla raccolta tecnologica e sistematica di informazioni generate da individui del tutto inconsapevoli della loro captazione da parte dei vari dipartimenti di polizia. Non è difficile scorgere in una simile prassi i caratteri propri della *dataveillance*, quali la focalizzazione sui dati, l'impiego di tecnologie e *dataset* all'avanguardia, il decentramento delle sedi adibite al monitoraggio, la trasparenza dei sorvegliati e il nascondimento dei sorveglianti. Essa, dunque, ben potrebbe essere pensata come prima e cruciale fase delle operazioni di polizia predittiva compiute dalle forze dell'ordine.

[37] Camaldo, 2025, 64 e 67.
[38] Ferguson, 2019, 499. Cfr. anche Camaldo, 2025, 65, e Basile, 2019, 11.
[39] Pietrocarlo, 2024, 15. Cfr. anche Meijer e Wessels, 2019, 1034, e Santaniello, 2019, 91-93.

Viceversa, l'attività che segue l'ottenimento delle previsioni algoritmiche si sostanzia in una serie di approcci tesi a far percepire la presenza degli operatori di polizia alle persone che si è previsto possano essere coinvolte in eventi criminali. Che si tratti di pattugliare assiduamente una zona ritenuta ad alta probabilità di reati o di ammonire direttamente gli individui inseriti all'interno di una lista di sospettati, le forze dell'ordine tendono ad adempiere la propria funzione deterrente servendosi degli *output* generati dai sistemi di *predictive policing* per monitorare fisicamente le persone da essi interessate, rendendole al contempo edotte della condizione di controllo in cui si trovano. A emergere, qui, sono i tratti propri della sorveglianza, la quale si è visto essersi storicamente manifestata anzitutto nella forma del pattugliamento preventivo operato dalla polizia londinese.

A unire queste due fasi vi è un collante imprescindibile: l'analisi algoritmica. Senza di essa, infatti, la mera raccolta di dati rappresenterebbe un'attività fine a se stessa, vista l'impossibilità di servirsi proficuamente delle informazioni immagazzinate facendo affidamento sulle sole, limitate, capacità umane. In tale ipotesi, nessun vantaggio ne trarrebbero le attività di polizia concretamente svolte, le quali si ritroverebbero nella situazione di doversi basare su una congerie infinitesimale di dati in assenza di una valida chiave di lettura degli stessi.

In questi termini, dunque, la polizia predittiva può intendersi come un'operazione complessa costituita da due fasi, una di *dataveglianza* e una di autentica sorveglianza, tra loro legate da un essenziale passaggio intermedio di analisi algoritmica. Per tale ragione, la *predictive policing* sembra rappresentare un esempio lampante di *dataveillance* funzionale alla sorveglianza o, detto altrimenti, di sorveglianza implementata attraverso la *dataveglianza*.

Come facilmente intuibile, pratiche tanto evolute a livello tecnologico non possono che comportare rischi altrettanto elevati sul piano procedimentale e, soprattutto, con riguardo agli effetti prodotti sulle persone destinate ad esserne interessate. Per meglio comprendere simili problematiche, si ritiene opportuno analizzare separatamente le criticità di cui soffrono i due summenzionati paradigmi di monitoraggio che concorrono a rendere possibile l'esperienza della polizia predittiva, ossia la sorveglianza (nella sua forma contemporanea di videosorveglianza) e la *dataveillance*.

3. Inefficacia e *chilling effect* nella videosorveglianza

Nonostante sia comunemente associata ad obiettivi virtuosi ed auspicabili nella loro realizzazione, la videosorveglianza ha da sempre rappresentato uno dei principali oggetti di diffidenza e disapprovazione da parte della critica prevalente.

Già diversi anni addietro, Chiara Fonio, esaminando lo specifico contesto della città di Milano, notava che, se da un lato le telecamere sono installate «con fini di deterrenza, incremento della percezione di sicurezza dei cittadini, miglioramento della vivibilità dei parchi e per ottimizzare gli interventi delle forze di polizia»[40], dall'altro lato «non ci sono dei dati inerenti [...] all'efficacia della videosorveglianza»[41]. Una simile discrasia dimostrerebbe, anzitutto, la mancanza di «un approccio critico che vada oltre i potenziali benefici», ovverosia di «un dibattito che vada oltre le mirabolanti capacità degli occhi elettronici che "tutto vedono e tutto possono"»; carenza, questa, che concorrerebbe a fondare, con tanto entusiasmo ma senza adeguata giustificazione, «il mito della sorveglianza = sicurezza»[42].

Le perplessità sollevate da Chiara Fonio in merito alla reale efficacia preventiva e securitaria delle videocamere sembrano diventare un'autentica certezza nel pensiero di Stefano Rodotà, il quale riteneva che la loro diffusione non servisse ad altro se non a determinare uno «spostamento della criminalità»[43] dalle aree soggette a videosorveglianza a quelle che ancora ne sono prive. In altri termini, non solo le telecamere rischiano di non essere effettivamente utili per la risoluzione delle problematiche in ragione delle quali vengono installate, ma tenderebbero addirittura a compiere una mera «operazione di rimozione»[44] che semplifica oltremodo la complessità del reale ed impedisce di cogliere le ragioni sociali, politiche ed economiche alla base di fenomeni che andrebbero compresi e affrontati, e non solamente allontanati: «la videosorveglianza non sempre "fa vedere" la realtà. Può oscurarla»[45]. Rassicura ma non cura.

Inoltre, nella letteratura scientifica è stato via via evidenziato che il ricorso alle videocamere non solo non permette di mantenere appieno la promessa di deterrenza e sicurezza che ne sorregge concettualmente l'installazione, ma addirittura che esso potrebbe costituire una fonte di incertezza per i consociati. A nessuno, infatti, è dato sapere chi si celi dietro un impianto di videosorveglianza[46], né tanto meno se tale soggetto (individuale o collettivo che sia) possegga davvero gli strumenti socio-culturali, oltre che tecnici, necessari per adempiere correttamente al proprio ruolo[47]. Per quanto sofisticata, peraltro, nessuna telecamera può dirsi del tutto al riparo dalla possibilità di

[40] Fonio, 2009, 103.
[41] *ivi*, 109.
[42] *ivi*, 114.
[43] Rodotà, 2004, 173.
[44] *ivi*, 179.
[45] *ivi*, 180.
[46] Cfr. Lyon, 1997, 132.
[47] Cfr. Fonio, 2009, 106.

attacchi esterni da parte di curiosi o malintenzionati[48], chiaramente invisibili agli occhi del cittadino. A ciò si aggiungono le incertezze relative alla durata dell'archiviazione delle registrazioni e alle modalità della loro visualizzazione[49], elementi, questi, che, come ha evidenziato Michele Bocchiola, concorrono a destare preoccupazione non tanto (o non solo) rispetto al fatto di essere ripresi, quanto piuttosto riguardo «l'utilizzo di quelle immagini»[50].

Davanti ad una telecamera, a fare da contraltare alla congerie di timori e dubbi ora brevemente sintetizzati sembra esservi una sola certezza: quella di essere visti[51], o meglio, quella di *poter* essere visti. Benché non manchi chi, come Wolfgang Sofsky, ritiene che la videosorveglianza rientri tra quelle forme di monitoraggio che, complice l'abitudine, non vengono più avvertite così intensamente dalla maggior parte delle persone[52], sembra difficile mettere in dubbio l'osservazione di quanti, come Stefano Rodotà, affermano che «adesso qualsiasi telecamera attira l'attenzione del più normale dei cittadini»[53]. Il fatto che la videosorveglianza sia generalmente accettata in virtù delle istanze securitarie a cui viene usualmente associata[54], oltre che la cospicua diffusione di videocamere all'interno di tessuti urbani e centri abitati[55], non anestetizzano del tutto la consapevolezza degli individui circa la presenza di simili sistemi di controllo nei luoghi da essi frequentati, né impediscono loro di notare di volta in volta i singoli dispositivi di monitoraggio (spesso ingombranti, appariscenti e indicati da apposita segnaletica). In altri termini, le persone generalmente notano la presenza di occhi elettronici, e quando vi si imbattono sanno bene di (poter) essere osservate.

La consapevolezza di essere inquadrati dai sistemi di videosorveglianza, unita all'incertezza circa il destino prossimo e futuro delle loro registrazioni, può costituire una minaccia per le libertà individuali e le pratiche democratiche.

Questo vale senz'altro nei Paesi contraddistinti dalla presenza di regimi più o meno illiberali. Josh Chin e Liza Lin, ad esempio, hanno raccontato come, nell'Uganda del presidente Yoweri Kaguta Museveni, la diffusione

[48] Cfr. Denardis, 2019, 78, e Greenfield, 2017, 47.
[49] Cfr. Brunton e Nissenbaum, 2016, 78.
[50] Bocchiola, 2014, 145.
[51] Cfr. Razac, 2012, 162.
[52] Cfr. Sofsky, 2010, 10.
[53] Rodotà, 2005, 18.
[54] Cfr. Zuccarini, 2009, 93.
[55] Sulla quantità e la densità di videocamere nelle maggiori metropoli mondiali cfr. Harari, 2024, 325. Sui progetti cinesi Skynet e Sharp Eyes che hanno condotto alla massiccia installazione di telecamere tanto nelle metropoli quanto nelle zone rurali cfr. Chin e Lin, 2022, 105. Sul numero di videocamere presenti a Londra cfr. Mayer-Schoneberg e Cukier, 2013, 203.

di «ghirlande di dissuasori antifurto» e di «nuovi gruppi di telecamere di sorveglianza» (c.d. *Safe City*), tutte targate Huawei, abbia costituito un serio problema per i rappresentanti delle opposizioni, i quali, se «un tempo si preoccupavano solo di non essere fisicamente pedinati», da qualche anno a questa parte hanno dovuto iniziare a «stare attenti anche a non fermarsi troppo a lungo in pubblico»[56].

Ma la videosorveglianza può sortire effetti negativi anche in contesti saldamente democratici, ove, non a caso, spesso si sviluppano movimenti di protesta proprio contro la dilagante presenza di videocamere[57]. Per comprendere in che cosa queste conseguenze pregiudizievoli si concretino, centrale è la nozione di *chilling effect*, che Federica Paolucci spiega come «una modificazione delle abitudini individuali per evitare di sottostare all'occhio indiscreto di una telecamera, pur di tutelare la nostra riservatezza»[58]. L'impatto di tale "effetto raggelante" è senz'altro ampio, e sarebbe quantomeno rischioso sottostimarlo. A livello individuale, Michele Bocchiola ha evidenziato come la dilagante diffusione della videosorveglianza, andando ad «invadere la privacy e, di conseguenza, limitare i comportamenti delle persone», comporti per ciò stesso «l'ovvia limitazione della libertà personale, che si abbia o meno qualcosa da nascondere»[59]. Sul piano sociale, invece, interessante è l'osservazione fatta da Simone Tulumello, secondo il quale un simile contesto, rafforzando «la sensazione dello spazio urbano come luogo pericoloso»[60], induce a «limitare la pratica di cittadinanza attiva», ovverosia la propensione delle persone a dare avvio o a prendere parte a manifestazioni, attivismo, proteste rituali e simili.

In sintesi, il crescente ricorso all'impiego di telecamere non solo non sembra contribuire in maniera significativa alla risoluzione delle problematiche determinate da condotte illecite, ma rischia addirittura di disincentivare comportamenti leciti, o persino auspicabili, anche in un contesto democratico rispettoso della persona e dei suoi diritti. Nello spasmodico tentativo di prevenire fenomeni criminali o pericolosi – e, forse, proprio in virtù di ciò -, la videosorveglianza corre il pericolo di condizionare indebitamente le abitudini e gli atteggiamenti degli individui, limitandone le libertà personali e inibendo pratiche collettive essenziali ad un regime politico propriamente democratico.

[56] Chin e Lin, 2022, 157.
[57] Cfr. Mitnik e Vamosi, 2023, 147; Ziccardi, 2022, 61; Brunton e Nissenbaum, 2016, 64.
[58] Paolucci, 2021, 214. Nel gergo legale di *common law*, *chilling effect* significa la refrattarietà ad esercitare un proprio diritto per paura di ripercussioni, un fenomeno generalmente amplificato dagli algoritmi: cfr. Büchi *et al.*, 2020.
[59] Bocchiola, 2014, 51-52.
[60] Tulumello, 2013, 34.

4. La *dataveillance* e i pericoli del *profiling*

Nel contesto attuale, il progresso tecnologico ha permesso a realtà *online* e dimensione *offline* di intrecciarsi quasi inscindibilmente tra loro, realizzando quella che Luciano Floridi ha da tempo definito *onlife*[61]. Ciò significa che un numero in costante crescita di abitudini personali e atteggiamenti quotidiani finisce per tradursi in lunghe ed impalpabili stringhe alfanumeriche, comunemente note come dati[62] e metadati[63]. Come si è visto in precedenza, essi rappresentano il principale oggetto – e, dunque, anche la fondamentale ragione di esistenza - della *dataveglianza*, la quale si propone anzitutto di raccoglierli e di immagazzinarli all'interno di *database* dalla capienza smisurata.

Il puro e semplice "possesso" di tali informazioni, tuttavia, non rappresenta in sé un effettivo vantaggio, né potrebbe garantire alcun reale beneficio qualora non si avesse a disposizione anche un qualche sistema algoritmico che, capace di operare ad una velocità e su basi di dati ben al di là delle limitate potenzialità umane, riesca a ordinarle ed organizzarle secondo una logica specifica. In altri termini, cattura e incameramento di informazioni non sono attività fini a se stesse. Esse rappresentano pratiche funzionali alla realizzazione della profilazione, che il GDPR (*General Data Protection Regulation*) definisce 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»[64]. Il *profiling* consiste, cioè, nell'utilizzo di sistemi algoritmici e di AI per aggregare e far interagire tra loro le informazioni precedentemente raccolte e immagazzinate, prima al fine di identificare degli ideal-tipi accomunati, ciascuno, dal possesso di caratteristiche omogenee, e poi allo scopo di procedere alla segmentazione delle persone attraverso il loro singolare inquadramento e la loro precisa attribuzione entro una delle specifiche categorie così determinate. Tracciare il profilo di un individuo costituisce un'attività a sua volta funzionale non solo a descrivere e comprendere le sue idee, la sua personalità e le sue condotte, ma anche a prevederle, in vista della successiva messa in atto di pratiche che riescano ad entrarvi in contatto in maniera efficace[65].

[61] Cfr. Floridi, 2017, 47 ss.
[62] Sulla nozione di dati cfr., tra i molti, Greenfield, 2017, 214.
[63] Sulla nozione di metadati cfr. Focarelli, 2015, 28. Sulla rilevanza dei metadati cfr. Mitnik e Vamosi, 2023, 25-27; Denardis, 2021, 82; Zuboff, 2019, 288-290.
[64] art. 4, n. 4, Reg. (UE) 2016/679.
[65] Sulla nozione di profilazione, sulle sue fasi e sulle sue finalità primarie cfr. Coniglione,

Scorgere i lati oscuri delle pratiche di *targetizzazione* non è sempre un'operazione agevole, soprattutto per l'impegnato e disattento utente medio, non sempre munito delle competenze minime necessarie a muoversi con accortezza nell'intricato ed interconnesso mondo digitale. Anzitutto, numerosi studiosi hanno evidenziato come le operazioni di raccolta delle informazioni vengano condotte con modalità strutturalmente funzionali ad abbassare il grado di attenzione dell'utente, come avviene con il ricorso sempre più frequente a prodotti della *gamification*[66]. A ciò si assomma quanto rilevato da Monica Zuccarini già diverso tempo addietro, ovverosia «il carattere invisibile dei processi di categorizzazione, selezione sociale, classificazione che sono effettuati tecnologicamente»[67] attraverso algoritmi muti e sulla base di dati del tutto impalpabili tanto nel loro movimento quanto nella loro stessa generazione. Da ultimo, non può certo sottostimarsi il fatto che tali attività di *targeting* siano foriere di evidenti comodità ed indubbi miglioramenti, talvolta a tal punto manifeste (e manifestate) da oscurare e silenziare completamente qualsivoglia possibile preoccupazione relativa alla tutela della privacy e dei dati personali. Per prima cosa, la profilazione è spesso sinonimo di prodotti personalizzati e vantaggi economici per il singolo individuo, il quale finisce spesso per rinunciare, felicemente ma inconsapevolmente, ad una quota più o meno consistente del proprio nebuloso diritto alla riservatezza per ottenere in cambio funzionalità tangibili, facilitazioni concrete, se non addirittura benefici monetizzabili[68]. Dal punto di vista sociale, invece, l'analisi delle informazioni e il tracciamento dei profili possono rivelarsi assai convenienti, o addirittura salvifici: Maria Orefice ne ha evidenziato i possibili utilizzi in ambito sanitario, ove possono contribuire a «diagnosticare una patologia e individuare la terapia curativa», a «produrre anche un risparmio di spesa», o addirittura a «salvare delle vite umane»[69]; Carlo Focarelli ne ha ricordato i pro «nel settore delle utenze» e «nel campo dei trasporti»[70]; Marco Delmastro e Antonio Nicita ne hanno mostrato l'uso positivo anche «nel settore bancario e finanziario»[71].

2023, 5; Han, 2023, 27; Mitnik e Vamosi, 2023, 61; Ziccardi, 2022, 35-37; Bazzoni, 2019, 639; Delmastro e Nicita, 2019, 37; O'Neil, 2017, 221; Maestri, 2015, 83-84; Mayer-Schoneberg e Cukier, 2013, 216; Rodotà, 2004, 174.

[66] Sulla *gamification* quale modalità operativa funzionale alla *dataveillance* cfr. Doctorow, 2024, 26; Perri, 2020, 30; Colamedici e Gancitano, 2021, 137; Zuboff, 2019, 230-231.

[67] Zuccarini, 2009, 98.

[68] Sul punto cfr. Coniglione, 2023, 5; Mitnik, 2023, 172; Varoufakis, 2023, 119; Chin e Lin, 2022, 121; Di Corinto, 2022, 32; Han, 2022, 10-11; Denardis, 2021, 87; Kaiser, 2019, 102-103; Greenfield, 2017, 28; Sofsky, 2010, 10.

[69] Orefice, 2018, 152-153.

[70] Focarelli, 2015, 51.

[71] Delmastro e Nicita, 2019, 16.

Tuttavia, il fatto che il *profiling* possa avere ricadute positive per i singoli individui e vantaggiose per l'intera collettività non deve indurre a tralasciare o sottovalutare i rischi che esso intrinsecamente comporta. Per comprenderli chiaramente, centrali sono le nozioni ormai classiche di *filter bubble* ed *echo chamber*, che Gabriele Giacomini definisce, rispettivamente, come «una bolla in cui [si] riceve solo informazioni che confermano ciò [in cui si] crede, [...] senza essere esposti a punti di vista differenti», e come «un ambiente chiuso che riflette se stesso, una stanza di specchi, una camera di risonanza in cui ognuno trova ciò che più gli piace e incontra le persone che hanno gli stessi suoi interessi [...]»[72].

Già di per sé, la creazione di simili bolle del filtro appare in contrasto con una nozione piena ed effettiva di dignità umana, posto che essa tende a reificare l'essere umano[73], trasformandolo in una mera fonte di dati da utilizzare per ottenere un profilo i cui contorni vengono tracciati bypassando completamente il consenso e la libertà di autodeterminazione del singolo soggetto destinato ad esserne, suo malgrado, titolare[74]. Ma c'è di più.

La reclusione virtuale di una persona all'interno di una camera dell'eco può provocare delle conseguenze considerevoli sulla sua vita, andando ben oltre la pur non irrilevante discriminazione di prezzi in base alla *willingness to pay* di ciascuno[75]. Da un lato, se è vero che sempre più attività umane sono destinate a svolgersi, in tutto o in parte, nella Rete o attraverso di essa, parimenti non è possibile negare che in tale ambiente le azioni e le scelte che un individuo è nella condizione di intraprendere sono solamente quelle messegli a disposizione dal sistema di volta in volta utilizzato, le quali, a propria volta, dipendono dall'attività di *targetizzazione* che vi sta dietro[76]. Dall'altro lato, l'impiego dell'AI nell'elaborazione dei *Big Data* ha reso possibile valutare complessivamente potenzialità e caratteristiche di ciascun soggetto, permettendo di attribuirvi un credito sociale, il quale potrebbe essere utilizzato per stabilire *a priori* quale candidato assumere o a chi garantire determinate prestazioni o l'accesso ad uno specifico mercato[77]. Come ha osservato Stefano Rodotà, è proprio in un contesto che offre possibilità diverse a persone differenti in ragione dei soli esiti di un *targeting* opaco e aprioristico che «s'insinua il germe di nuove discriminazioni, nasce il cittadino non più libero, ma "profilato", prigioniero di meccanismi che non sa o non può

[72] Giacomini, 2018, 137. I concetti di *filter bubble* ed *echo chamber* sono in uso oramai da diversi anni: il primo viene fatto risalire a Pariser, 2011, il secondo a Barberá *et al.*, 2015.
[73] Cfr. Rodotà, 2014, 27-28.
[74] Cfr. Maestri, 2015, 86.
[75] Cfr. Delmastro e Nicita, 2019, 81.
[76] Cfr. *ivi*, 84, e Greenfield, 2017, 40.
[77] Cfr. Sarra, 2022b, 34, e Pin, 2021, 56.

controllare»[78]. Senza dimenticare il fatto che tale classificazione potrebbe essere disposta sulla base di dati o processi errati, incompleti o affetti da un qualche tipo di *bias*[79].

Rinchiuso all'interno della propria bolla del filtro, inoltre, l'individuo diviene progressivamente bersaglio di contenuti e informazioni che l'algoritmo ha ritenuto in linea con le idee e le preferenze emerse a seguito dell'analisi dei dati raccolti. Ciò significa che, anche se errate o frutto della supina accettazione di un pregiudizio infondato, le opinioni individuali sono destinate a radicarsi ben oltre ciò che avviene in virtù di meccanismi psicologici e neurologici[80], posto che sarà sempre più difficile per esse imbattersi in visioni opposte, divergenti o anche solo capaci di metterle parzialmente in discussione[81]. Questo contesto di forte autoreferenzialità comporta una pericolosa condizione di isolamento intellettuale della persona[82], foriera di pregiudizievoli ricadute anche per la comunità e il panorama politico. Cass R. Sunstein è stato tra i più chiari a rilevare che «l'isolamento e la personalizzazione sono soluzioni a problemi autentici, ma diffondono falsità e incentivano la polarizzazione e la frammentazione»[83], entrambi fenomeni problematici per un contesto democratico che, per definizione, necessita di un costante confronto dialogico[84] e che poggia sulla logica della *concordia discors*[85].

Detto altrimenti, la *dataveillance* rischia in numerosi casi di porsi come anticamera (necessaria) di un processo più ampio che considera le persone solamente nella loro dimensione datificata, e che, profilandole, le isola in ambienti invisibili ed autoreferenziali, i quali, se da un lato mirano a discriminare le opportunità a disposizione dei soggetti in ragione delle infor-

[78] Rodotà, 2014, 39. Cfr. anche Pin, 2021, 57.

[79] Cfr. Harari, 2024, 318; O'Neil, 2017, 226; Focarelli, 2015, 53.

[80] Il riferimento qui è anzitutto alle euristiche e distorsioni cognitive, tra le quali spiccano, *in primis*, il *confirmation bias* (cfr. Antonazzi, 2020, 194) e l'effetto gregge (cfr. Giacomini, 2018, 128-129).

[81] Cfr. Coniglione, 2023, 10; De Fabritiis, 2023, 133; Sarra, 2022a, 94-95; Barberis, 2020, 159; Lagioia e Sartor, 2020, 87; Delmastro e Nicita, 2019, 98 e 102; Giacomini, 2018, 62.

[82] Cfr. Delmastro e Nicita, 2019, 111, e Giacomini, 2018, 59-60.

[83] Sunstein, 2017, 15. Gabriele Giacomini ha spiegato bene la differenza semantica tra questi due fenomeni, spesso connessi ed abbinati ma non del tutto sovrapponibili: «per frammentazione si intende l'aumento del numero di fonti di informazione disponibili, mentre per polarizzazione si intende una crescente distanza nelle posizioni di coloro che si informano presso fonti diverse»: Giacomini, 2018, 58. Proprio Giacomini ha descritto questa condizione in termini di «incastellamento» (*ivi*, 116-117), mentre Mauro Barberis ha parlato di «tribalizzazione» (Barberis, 2020, 138-139).

[84] Sulla dannosità di polarizzazione e frammentazione per il dibattito pubblico cfr. Colamedici e Gancitano, 2021, 42; Barberis, 2020, 138-139; Lagioia e Sartor, 2020, 100; Giacomini, 2018, *passim*.

[85] Sulla nozione di *concordia discors* come «consenso imperfetto ma che è corroborato dal dissenso», e su come essa sia circondata da dinamiche che ne impediscono una piena realizzazione, cfr. *ivi*, 116-117.

mazioni possedute sul loro conto, dall'altro lato costituiscono un ostacolo di non poco conto all'esercizio delle libertà individuali e collettive, nonché all'effettivo espletamento dell'essenza dialogica del regime democratico.

5. La *predictive policing* tra *dirty data*, opacità algoritmica e *chilling effect* "mirato"

Analizzate le insidie che si annidano nelle due principali forme odierne di monitoraggio, l'attenzione deve ora nuovamente focalizzarsi sulle pratiche di polizia predittiva, le quali non possono certo ritenersi esenti da pericoli e problematiche. La dottrina dedicatasi al fenomeno della *predictive policing*, infatti, ne ha da sempre messo in evidenza i rischi intrinseci, e continua tutt'ora a sottolinearli, generalmente facendo seguire a tali rilevazioni la richiesta di interventi normativi volti a scongiurarli.

Nella letteratura scientifica, le principali criticità sono state rinvenute già nella fase di raccolta dei dati destinati, in un momento successivo, ad essere utilizzati nell'analisi algoritmica compiuta in vista dell'ottenimento delle previsioni.

Con riguardo alle tecnologie impiegate per compiere tale operazione, ad esempio, Simone Lonati ha ricordato che esse «sono molto eterogenee» e vanno «dall'analisi dei *social network* al riconoscimento facciale», con il risultato di suscitare sin da subito «forti perplessità in tema di *privacy* dei cittadini»[86]. Spostando l'attenzione dalla raccolta in sé, e dagli strumenti attraverso i quali si esplica, al suo oggetto, ovverosia i dati, Elisabetta Pietrocarlo ha evidenziato che la loro qualità potrebbe essere inficiata tanto da «possibili errori nelle fasi di raccolta, selezione e inserimento nel sistema», quanto da lacune che potrebbero impedire al *dataset* di essere «effettivamente rappresentativo della realtà»[87] rispetto alla quale si vanno cercando predizioni. Inoltre, condividendo e facendo propria un'argomentazione assai diffusa nella critica, Beatrice Perego ha segnalato che «pregiudizi personali o culturali non intenzionali possono "contaminare" i dati»[88], finendo poi per moltiplicarsi e amplificarsi in sede di analisi algoritmica[89]. Se, da un lato, una simile dinamica determina inevitabilmente la messa in discussione della

[86] Lonati, 2022, 305. Cfr. Basile, 2022, 5; Perego, 2022, 452-453; Meijer e Wessels, 2019, 1036.
[87] Pietrocarlo, 2024, 11. Sul tema della qualità dei dati cfr. Peluso, 2022. Sulle imprecisioni e carenze dei *database* utilizzati dai sistemi di polizia predittiva cfr. Lonati, 2022, 305, e Ferguson, 2017a, 1145-1147. Errori ed inesattezze potrebbero essere anche il risultato di una manipolazione o deformazione intenzionale: cfr. Camaldo, 2025, 71, e Basile, 2022, 5.
[88] Perego, 2022, 459. Cfr. anche Pietrocarlo, 2024, 11; Lonati, 2022, 305; Mayson, 2019, 2218 ss.; Burchard, 2019, 1932 ss.; Santaniello, 2019, 93-94.
[89] Cfr. Pietrocarlo, 2024, 13; Perego, 2022, 460-464; Mugari e Obioha, 2021, 10.

presunta neutralità e della pretesa imparzialità di algoritmi che, alla fine, si rivelano distorti da *bias* personali e ideologie di parte[90], dall'altro lato essa rischia di generare effetti paradossali quali quello del *feedback loop*[91].

Errori, lacune e pregiudizi, dunque, sono tra le principali problematiche passibili di annidarsi tra i dati utilizzati dai sistemi di polizia predittiva, i quali, per ciò stesso, vengono talvolta definiti *dirty data*. Si tratta di profili estremamente infidi e pericolosi, non solo perché difficili da individuare e isolare, ma anche e soprattutto in ragione del fatto che le distorsioni che inficiano ciò che viene assunto come *input* non si neutralizzano autonomamente attraverso l'analisi algoritmica, conducendo, viceversa, ad *output* falsati, imprecisi, inattendibili o del tutto errati[92]. E ciò che più inquieta è che simili risultati, per quanto intaccati nella loro validità, sono destinati ad essere comunque impiegati per indirizzare le operazioni delle forze dell'ordine, le quali rischiano per ciò stesso di orientarsi verso falsi positivi[93] o di tradursi in pratiche discriminatorie[94] ancor più radicate in quanto supportate da una giustificazione ammantata di scientificità[95].

L'altro grande nodo problematico della *predictive policing* è stato rinvenuto dalla dottrina con riguardo ai processi di analisi algoritmica di cui essa si vale per tramutare l'agglomerato informe e disorganico dei dati raccolti in previsioni precise e dotate di immediata operatività pratica.

Anche in un ambito così delicato come quello della polizia predittiva, gli algoritmi e i procedimenti da essi compiuti si caratterizzano per un elevato grado di opacità[96]. Tale fenomeno dipende anzitutto da quelle che Elisabetta Pietrocarlo ha definito «ragioni tecniche», e che si sostanziano nel «*black box problem* dovuto al fatto che gli algoritmi basati sull'intelligenza artificiale si distaccano dalle istruzioni iniziali per apprendere autonomamente»[97]. Tuttavia, una simile opacità, per così dire, naturale ed inevitabile spesso fi-

[90] Cfr. Perego, 2022, 452, e Noto La Diega, 2018b, 33.

[91] Cfr. Pietrocarlo, 2024, 14. Anche Mauro Santaniello parla di *feedback loop* (cfr. Santaniello, 2019, 93), mentre Lucio Camaldo parla di *self-fulfilling prophecies* (cfr. Camaldo, 2025, 71), Fabio Basile parla di *profezia che si auto-avvera* (cfr. Basile, 2022, 8), Simone Lonati parla di *confirmation feedback loop* (cfr. Lonati, 2022, 308-309), e Beatrice Perego riprende l'espressione *ratchet effect* (Perego, 2022, 460-461).

[92] Cfr. Pietrocarlo, 2024, 11.

[93] Cfr. *ivi*, 13; Bonfanti, 2018, 207; European Parliament, *Report on fundamental rights implications of big data: privacy, data protection, nondiscrimination, security and law-enforcement*, 2016/2225 (INI), Committee on Civil Liberties, Justice and Home Affairs, 20 febbraio 2017, par. M.

[94] Cfr. Camaldo, 2025, 70-71; Basile, 2022, 8; Perego, 2022, 460; Manes, 2020; Ferguson, 2019, 492 e 504; Meijer e Wessels, 2019, 1036; Richardson, Schultz e Crawford, 2019, 192 ss.; Bonfanti, 2018, 207.

[95] Cfr. Perego, 2022, 462.

[96] Cfr. *ivi*, 458-459, e Meijer e Wessels, 2019, 1036.

[97] Pietrocarlo, 2024, 12; Perego, 2022, 459; Noto La Diega, 2018a, 4 ss.

nisce per essere acuita dal fatto che, per usare le parole di Mauro Santaniello, «gran parte dei sistemi in uso [...] sono prodotti da compagnie private, che custodiscono gelosamente i propri codici sorgente per evitare che questi vengano duplicati o parzialmente copiati dai propri concorrenti», e che archiviano ed elaborano in prima persona «i dati di cui si nutre il sistema di *machine learning*»[98].

L'opacità dei processi algoritmici e, conseguentemente, delle previsioni che da essi emergono determina un difetto di trasparenza che danneggia coloro che, loro malgrado, ne sono destinatari. Se da un lato questi ultimi risultano spesso sprovvisti di strumenti giuridici adeguati ad una efficace contestazione delle decisioni e pratiche intraprese nei loro confronti su base algoritmica[99], dall'altro lato è stato evidenziato che, anche qualora simili rimedi fossero effettivamente previsti ed operativi, l'impossibilità di pervenire ad una spiegazione completa del funzionamento e degli esiti dei procedimenti algoritmici continuerebbe a determinare una mancanza di *accountability*[100].

I profili problematici della *predictive policing* qui sintetizzati sono quelli che maggiormente sono stati evidenziati e continuano ad essere messi in luce dalla letteratura scientifica prevalente. Appare evidente che essi attengono perlopiù all'attività di raccolta dei dati, nonché al momento di analisi algoritmica, ad essa immediatamente successivo e teleologicamente correlato.

Tuttavia, come si è avuto modo di mostrare in precedenza, la polizia predittiva rappresenta un fenomeno composito, costituito da una (prima) fase di *dataveglianza* e da una (seconda) fase di sorveglianza, tra loro unite da quel legame essenziale costituito dal processo algoritmico. La disamina delle principali criticità connesse alla videosorveglianza in quanto forma più evoluta e oggi più diffusa di sorveglianza, ha dimostrato che quest'ultima non può certo dirsi esente da possibili derive pregiudizievoli, tra le quali spicca quella che si estrinseca nella produzione del *chilling effect* nei confronti degli individui e delle comunità che essi concorrono a comporre.

Ebbene, ciò che pare talvolta sfuggire alla dottrina è il fatto che, proprio in quanto destinata ad estrinsecarsi anche ed in ultima istanza in un'attività di autentica sorveglianza, la *predicitve policing* corre il rischio di deter-

[98] Santaniello, 2019, 94. Cfr. anche Camaldo, 2025, 72; Pietrocarlo, 2024, 12-13; Basile, 2022, 9; Lonati, 2022, 306; Perego, 2022, 459; Hung, e Yen, 2021, 166 ss.; Joh, 2017. Andrew Ferguson ha ricordato che «some of the technologies are proprietary, owned by private entities that sell and market their services in competitive market. Some of the technologies are based out of universities and are provided free or through a licensing arrangement. And, a few technologies are associated with large multinational technology firms with deep financial pockets»: Ferguson, 2019, 492-493.

[99] Cfr. Pietrocarlo, 2024, 14.

[100] Cfr. *ivi*, 13; Meijer e Wessels, 2019, 1036; Santaniello, 2019, 96; Ferguson, 2017a, 1169.

minare un "effetto congelante" nei confronti dei destinatari delle previsioni algoritmiche[101]. Addirittura, il *chilling effect* potenzialmente prodotto dalle pratiche di polizia predittiva potrebbe rivelarsi ancora più infido e dannoso rispetto a quello determinato dalla videosorveglianza. Infatti, mentre l'"effetto raggelante" prodotto da quest'ultima appare generale e indiscriminato, data la natura oramai ubiquitaria degli occhi elettronici, quello dipendente da sistemi di *predictive policing* è destinato a prodursi solo nei confronti di determinati soggetti o gruppi di individui. Nel caso dei *place-based systems*, infatti, il pattugliamento delle forze dell'ordine va moltiplicandosi soltanto rispetto alle aree considerate a maggior rischio di criminalità e, inevitabilmente, a coloro che vi abitano, i quali potrebbero vivere con insofferenza una presenza tanto massiccia di personale addetto al loro monitoraggio. Con riguardo ai *person-based systems*, invece, solamente i soggetti algoritmicamente identificati come più probabili autori di futuri reati vengono raggiunti dalla polizia e messi in guardia circa il fatto che essi, oltre ad andare incontro ad un aggravio sanzionatorio in caso di effettiva commissione di un illecito, saranno oggetto di una sorveglianza più stringente e meno clemente. In altri termini, ciò che potrebbe determinare il ricorso diffuso a pratiche di polizia predittiva non è soltanto un *chilling effect*, ma un *chilling effect* mirato e, quindi, potenzialmente discriminatorio, atteso anche il fatto che l'attività di sorveglianza compiuta nell'ambito della *predictive policing* segue l'impiego di dati generalmente affetti da *bias* ed errori e l'utilizzo di algoritmi opachi e tendenti ad amplificare i pregiudizi umani.

6. Alcune considerazioni conclusive

Quello della sorveglianza rappresenta un fenomeno tanto connaturato alla realtà del consorzio umano quanto articolato e complesso, e provare a tracciarne i confini concettuali costituisce un'impresa ardua, qualsiasi sia il contesto scientifico attraverso il quale ci si approssima ai *surveillance studies*. Una simile presa di coscienza, tuttavia, non deve fungere da comoda giustificazione per desistere da ogni possibile tentativo in tale direzione.

La nozione di sorveglianza si presenta come sfuggente anche e soprattutto in virtù della sua natura cangiante, della sua abitudine, cioè, a mutare forma

[101] Fabio Basile sembra aver colto almeno in parte questa criticità nel momento in cui ha rilevato che «questi sistemi sollecitano una prevenzione dei reati attraverso [...] una sorta di "militarizzazione" nella sorveglianza di determinate zone o di determinati soggetti», sebbene questo fenomeno venga valorizzato in una chiave differente, ancorché non meno importante, ovverosia quella di impedire di «mirare alla riduzione del crimine attraverso un'azione rivolta, a monte, ai fattori criminogeni»: Basile, 2022, 8-9. Cfr. anche Camaldo, 2025, 71.

e finalità a seconda del periodo storico e del contesto sociale, politico ed economico nel quale si trova ad operare. Preso atto di tale qualità camaleontica, nel presente contributo si è cercato di avvicinarsi ad una definizione di sorveglianza dapprima affondando lo sguardo nella sua radice etimologica e nelle sue prime manifestazioni storiche di epoca moderna, per poi confrontare quanto così emerso con una nozione che, oramai da qualche decennio, è stata adottata dalla dottrina prevalente come paradigma delle attività di monitoraggio operanti nelle società tecnologiche contemporanee, ovverosia quella di *dataveglianza*. Da tale raffronto sono risultati due modelli teorici tra loro distinti non solo per oggetto e modalità operative, ma anche per criticità: quello, appunto, della *dataveillance* definito da Roger Clarke, e quello della sorveglianza, per così dire, tradizionale, la quale sembra oggi rivivere soprattutto nella realtà della videosorveglianza.

Benché una simile separazione concettuale possa essere foriera di qualche utilità nella lettura delle variegate dinamiche di monitoraggio, nonché nell'individuazione dei loro elementi caratterizzanti, pare opportuno tenere a mente che essa non può dirsi così netta nella realtà concreta, e soprattutto in quella attuale. Edward Snowden, ad esempio, ha rilevato come, già nel 2011, iniziassero a circolare telecamere che, integrate con AI e riconoscimento facciale, non si limitavano alla mera registrazione delle immagini, ma si spingevano fino al tracciamento dei movimenti delle persone e all'elaborazione di determinate categorie di dati[102]. Shoshana Zuboff, invece, ha ricordato il c.d. *chilling effect* esteso, ovverosia l'autocensura posta in essere *offline* per evitare che talune informazioni prodotte nel mondo reale possano essere captate e rese oggetto di osservazione *online*.[103] In altri termini, soprattutto nel contesto tecnologico odierno, sorveglianza e *dataveglianza* si configurano come due fenomeni tra loro interconnessi e tutt'altro che separati l'uno dall'altro, destinati ad interagire tra loro e a rafforzarsi vicendevolmente.

Un esempio evidente di tale reciproca operatività è stato rinvenuto in quell'esperienza che viene complessivamente definita come polizia predittiva. Al netto delle molteplici specificità che contraddistinguono le sue varianti, essa si sostanzia sempre in una prima fase di monitoraggio e immagazzinamento di dati afferenti a categorie prestabilite (*dataveillance*), seguita da un processo di analisi algoritmica funzionale a tramutare le informazioni previamente acquisite in previsioni specifiche, poi utilizzate per orientare l'attenzione e la presenza delle forze dell'ordine verso determinate aree o persone (sorveglianza), perlopiù a scopo di deterrenza. Nell'ambito della *predictive policing*, dunque, sorveglianza e *dataveglianza* non si limitano ad

[102] Cfr. Snowden, 2019, 196-197.
[103] Cfr. Zuboff, 2019, 488.

interagire tra loro: esse si susseguono secondo un ordine preciso ed inalterabile, sicché il monitoraggio dei dati rinviene il proprio orizzonte e il proprio obiettivo esattamente nell'implementazione delle attività di controllo locale e personale[104].

L'ingresso nel mondo della polizia predittiva ha permesso, inoltre, di rilevare che, allorquando *dataveillance* e sorveglianza entrano in contatto tra loro, le rispettive criticità non necessariamente finiscono per eludersi o frenarsi a vicenda. Da un lato, si è visto come la gran parte delle problematiche riscontrate dalla dottrina nei sistemi di *predictive policing* sia pressoché sovrapponibile a (una parte di) quelle generalmente rilevate con riguardo alla *dataveglianza* e all'analisi algoritmica che la segue, ovverosia, su tutti, la presenza di *bias* ed errori nei set di dati raccolti ed immagazzinati, e l'opacità tecnica ed economica degli algoritmi chiamati a trattarli. Dall'altro lato, è emerso che, in quanto destinata ad estrinsecarsi in forme di vera e propria sorveglianza, la polizia predittiva corre il rischio di produrre un autentico *chilling effect*, analogo a quello generato dalla videosorveglianza, ma dai contorni potenzialmente ancor più pericolosi in quanto destinato a toccare soltanto alcuni soggetti o gruppi di individui, previamente identificati sulla base di informazioni e procedure affette da logiche discriminatorie, se non addirittura amplificative delle stesse. Insomma, quando *dataveillance* e sorveglianza entrano in dialogo all'interno di un medesimo sistema, anche le rispettive problematiche tendono a interagire tra loro, con esiti che oscillano tra la conservazione delle rispettive problematiche e la loro vicendevole implementazione.

Ciò non significa, ovviamente, che la *predictive policing* sia soltanto un meccanismo per innalzare all'ennesima potenza i rischi insiti nelle forme odierne di monitoraggio. Sorveglianza e *dataveglianza* possiedono senz'altro anche potenzialità benefiche, e i sistemi di polizia predittiva si propongono di valersene al fine di perseguire obiettivi indubbiamente meritevoli, quali una gestione più efficiente delle risorse materiali ed umane a disposizione delle forze dell'ordine, l'affermazione di pratiche di polizia più accurate ed oggettive e, soprattutto, una maggiore efficacia nella prevenzione della criminalità. La vera sfida, dunque, risiede proprio nella difficoltà di comprendere se ed in quali termini sia possibile assoggettare il fenomeno della *predictive policing* ad un regime giuridico che le permetta di mantenere, almeno

[104] Da evidenziare è, inoltre, il fatto che, nell'ambito della *predictive policing*, *dataveglianza* e sorveglianza tendono a creare un moto circolare che si auto-alimenta, posto che i dati raccolti nel corso delle attività di sorveglianza sono destinati ad essere impiegati nelle successive operazioni di *dataveillance* e analisi algoritmica. Si veda quanto detto *supra* in tema di *feedback loop*.

in parte, le promesse che essa porta con sé, impedendole altresì di scivolare verso derive indesiderate ma tutt'altro che improbabili.

La regolazione della polizia predittiva nelle aree dove esse risulta essersi diffusa non può certo dirsi omogenea, sebbene ispirata a principi generali spesso ricorrenti o coincidenti. Mentre negli Stati Uniti si registra un certo immobilismo da parte dei *policy-makers*[105], nel contesto euro-unitario[106] i *place-based systems* sono stati assoggettati alla disciplina dettata per i sistemi di IA ad alto rischio[107], laddove i *person-based systems* sono generalmente vietati, a meno che non vengano impiegati al solo fine di fornire sostegno entro un processo decisionale già imperniato su una valutazione umana fondata su un ragionevole sospetto a propria volta basato su fatti oggettivi e verificabili[108]. Offrendo una ricostruzione della polizia predittiva attraverso le categorie di sorveglianza e *dataveglianza*, attraverso il presente contributo è emersa una problematica poco trattata tanto dalla dottrina quanto sul piano normativo, ma che sembra percorrere trasversalmente la variegata realtà della *predictive policing*, la cui natura composita si dimostra foriera di criticità altrettanto complesse.

Bibliografia

Algeri, L. (2021). 'Intelligenza artificiale e polizia predittiva', in *Diritto penale e processo* 6: 724-734.

Antonazzi, M. (2020). 'La negoziazione cognitiva' in C. Sarra e F. Reggio, *Diritto, Metodologia Giuridica e Composizione del Conflitto*, 181-217. Milano: Primiceri.

Barberá, P., Jost, J.T., Nagler, J., Turker, J.A., e Bonneau, R. (2015). 'Tweeting from Left to Right: Is Online Political Communication More than an Echo Chamber?', in *Psychological Science* 26, 10: 1531-1542.

Barberis, M. (2020). *Come internet sta uccidendo la democrazia*. Milano: Chiarelettere.

[105] Cfr. Silverman, 2023, 17 ss. Tale stato di *deregulation*, tuttavia, risulta essere parzialmente bilanciato sia dalle reazioni decise di organizzazioni non governative come l'American Civil Liberties Union (ACLU) (sul cui operato si vedano Joh, 2022, 13 ss., e Ferguson, 2021, 250 ss.), sia da interventi di più ampio respiro, come il Blueprint for an AI Bill of Rights. Making Automated Systems Work for the Amenican People pubblicato nel 2022 dall'Office of Science and Technology Policy (OSTP) della Casa Bianca (per un'analisi del quale si rinvia a Pietrocarlo, 2023, 28-31).

[106] Per una ricostruzione critica e documentata della collocazione ricoperta dai sistemi di polizia predittiva all'interno della disciplina dettata dall'*AI Act* nel corso dell'iter che ha portato, infine, al suo testo definitivo cfr. Pietrocarlo, 2024, 16-23.

[107] Cfr. art. 59, Reg. 1689/2024/UE, e Allegato III, par. 6.

[108] Cfr. art. 5, lett. d), e cons. 42, Reg. 1689/2024/UE.

Basile, F. (2019). 'Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine', in *Diritto penale e uomo*: 1–33.

Basile, F. (2022). 'Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione' in G. Balbi, F. De Simone, A. Esposito e S. Manacorda (a cura di), *Diritto penale e intelligenza artificiale. «Nuovi scenari»*, 1-25. Milano: Giappichelli Editore.

Bazzoni, G. (2019). 'La libertà di informazione e di espressione del pensiero nell'era della democrazia virtuale e dei global social media', in *Diritto di Internet* 4: 635–643.

Benbouzid, B. (2019). 'To predict and to manage. Predictive policing in the United Stated', in *Big Data & Society*: 1-13.

Bocchiola, M. (2014). *Privacy. Filosofia e politica di un concetto inesistente*. Roma: LUISS University Press.

Bonfanti, A. (2018). 'Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali', in *MediaLaws* 3: 206–218.

Bratton, W.J., e Malinowski, S.W (2008). 'Police Performance Management in Practice. Taking COMPSTAT to the Next Level', in *Policing: A Journal of Policy and Practice* 2, 3: 259-265.

Brunton, F, e Nissenbaum, H. (2016). *Offuscamento. Manuale di difesa della privacy e della protesta*. Fano: Eretica Speciale.

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., Viljoen, S. (2020). 'Chilling Effect of Profiling Activities: Mapping the Issues', in *Computer Law & Security Review* 36: 1-36.

Burchard, C. (2019). 'L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società', in *Rivista Italiana di Diritto e Procedura Penale* 62, 4: 1909-1942.

Camaldo, L. (2025). 'Intelligenza artificiale e investigazione penale predittiva', in F. Basile, M. Biasi, L. Camaldo, G. Caneschi, B. Fragasso e D. Milani (a cura di), *Intelligenza artificiale. Diritto, giustizia, economia ed etica*, 61-83. Milano: Giappichelli Editore.

Chin, J., e Lin, L. (2022). *Stato di sorveglianza. La via cinese verso una nuova era del controllo sociale*. Torino: Bollati Boringhieri.

Clarke, R. (1988). 'Information Technology and Dataveillance', in *Communication of the ACM* 31, 5: 498–512.

Colamedici, A., e Gancitano, M. (2021). *L'alba dei nuovi dèi. Da Platone ai big data*. Milano: Mondadori.

Coniglione, C. (2023). 'L'utilizzo dei big data in ambito politico-elettorale e il loro impatto sulla democrazia rappresentativa', in *Nomos. Le attualità del diritto* 1: 1–14.

De Fabritiis, A. (2023). 'Social network e capitalismo della sorveglianza: i pericoli per la democrazia e l'antidoto di una visione antropologica cristiana', in *Prospettiva Persona · Prospettiva Logos* 120, 2: 131–142.

Delmastro, M., e Nicita, A. (2019). *Big data: come stanno cambiando il nostro mondo*. Bologna: Il Mulino.

Denardis, L. (2021). *Internet in ogni cosa*. Roma: Luiss University Press.

Di Corinto, A. (2022). 'Data commons: privacy e cybersecurity sono diritti umani fondamentali', in *Rivista Italiana di Informatica e Diritto* 1: 31–37.

Di Nicola, A., Espa, G., Bressan, S., Dickson, M.M., e Nicolamarino, A. (2014). 'Metodi statistici per la predizione della criminalità. Rassegna della letteratura su predictive policing e moduli di data mining', in *eCrime Working Papers* 2: 1-35.

Doctorow, C. (2024). *Come distruggere il capitalismo della sorveglianza*. Milano: Mimesis.

Egbert, S. (2018). 'About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany', in *European Journal for Security Research* 2, 3: 95-114.

Ferguson, A.G. (2017a). 'Policing Predictive Policing', in *Washington University Law Review* 94, 5: 1109-1189.

Ferguson, A.G. (2017b). *The Rise of Big Data Policing. Surveillance, Race, and The Future of Law Enforcement*. New York: New York University Press.

Ferguson, A.G. (2019). 'Predictive Policing Theory' in T. Rice Lave e E.J. Miller (eds), *The Cambridge Handbook of Policing in the United States*, 491-510. Cambridge: Cambridge University Press.

Ferguson, A.G. (2021). 'Surveillance and the Tyrant Test', in *The Georgetown Law Journal* 110, 2: 205-290.

Fioriglio, G. (2015). 'Controllo e sorveglianza nella società dell'informazione', in *Studi sulla questione criminale* X, 2–3: 7–23.

Floridi, L. (2017). *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*. Milano: Raffaello Cortina Editore.

Focarelli, C. (2015). *La privacy. Proteggere i dati personali oggi*. Bologna: Il Mulino.

Fonio, C. (2006). 'Oltre il Panopticon? Foucault e la videosorveglianza', in *Studi di Sociologia* 44, 2: 267-276.

Fonio, C. (2007). *La videosorveglianza. Uno sguardo senza volto*. Milano: FrancoAngeli.

Fonio, C. (2009). 'Gli occhi elettronici e la retorica della sorveglianza. Il caso di Milano' in D. Calenda e C. Fonio (a cura di), *Sorveglianza e società*, 101-116. Acireale-Roma: Bonanno Editore.

Ganascia, J.-G. (2010). 'The generalized sousveillance society', in *Social Science Information* 3, 3: 1-19.

Giacomini, G. (2018). *Potere digitale. Come Internet sta cambiando la sfera pubblica e la democrazia*. Milano: Meltemi.

Greenfield, A. (2017). *Tecnologie radicali. Il progetto della vita quotidiana*. Torino: Einaudi.

Han, B.-C. (2023). *Infocrazia. Le nostre vite manipolate dalla rete*. Torino: Einaudi.

Harari, Y.N. (2024). *Nexus. Breve storia delle reti di informazione dall'età della pietra all'AI*. Milano: Bompiani.

Hung, T.-W., e Yen, C.-P. (2021). 'On the Person-Based Predictive Policing of AI', in *Ethics and Information Technology* 23: 165-176.

Joh, E.E. (2017). 'The Undue Influence of Surveillance Technology Companies on Policing', in *New York University Law Review Online*: 19-47.

Joh, E.E. (2022). 'Ethical AI in American Policing', in *Notre Dame Journal on Emerging Technologies* 3, 2: 262-287.

Kaiser, B. (2019). *La dittatura dei dati. La talpa di Cambridge Analytica svela come i big data e i social vengono usati per manipolarci e minacciare la democrazia*. Milano: HarperCollins.

Lagioia, F., e Sartor G. (2020). 'Profilazione e decisione algoritmica: dal mercato alla sfera pubblica', in *federalismi.it* 11: 85–110.

Lonati, S. (2022). 'Predictive policing: dal disincanto all'urgenza di un ripensamento', in *MediaLaws* 2: 302–316.

Lyon, D. (1997). *L'occhio elettronico. Privacy e filosofia della sorveglianza*. Milano: Feltrinelli.

Lyon, D. (2002). 'Editorial. Surveillance Studies: Understanding visibility, mobility and the phenetic fix', in *Surveillance & Society* 1, 1: 1–7.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, D. (2022). 'Surveillance', in *Internet Policy Review* 11, 4: 1–19.

Maestri, E. (2015). *Lex informatica. Diritto, persona e potere nell'età del cyberspazio*. Napoli: Edizioni Scientifiche Italiane.

Manes, V. (2020). 'L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia', in *Discrimen*: 1-22.

Marx, G.T. (2015). 'Surveillance Studies', in *International Encyclopedia of the Social & Behavioral Sciences* II: 733–741.

Mayer-Schoneberg, V., e Cukier, K. (2013). *Big data: una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*. Milano: Garzanti.

Mayson, S.G. (2019). 'Bias In, Bias Out', in *The Yale Law Journal* 128: 2218-2300.

Meijer, A., e Wessels, M. (2019). 'Predictive Policing: Review of Benefits and Drawbacks', in *International Journal of Public Administration* 42, 12: 1031–1039.

Michetti, M. (2023). 'Sorveglianza, Rivoluzione tecnologica e tutela dei diritti fondamentali', in *Dirittifondamentali.it* 3: 546–579.

Mitnik, K.D., e Vamosi, R. (2023). *L'arte dell'invisibilità. Il più famoso hacker del mondo insegna come sparire nell'era in cui social media e big data stanno uccidendo la privacy*. Milano: Apogeo.

Mugari, I., e Obioha, E.E. (2021). 'Predictive policing and Crime Control in The United States of America and Europe. Trends in a Decade of Research and the Future of Predictive Policing', in *Social Science* 10, 6: 1-14.

Noto La Diega, G. (2018a). 'Against Algorithmic Decision-making', in *Northcolumbia Legal Studies Working Paper Series*: 1-7.

Noto La Diega, G. (2018b). 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information', in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 9, 1: 3-34.

O'Neil, C. (2017). *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia*. Milano: Giunti-Bompiani.

Orefice, M. (2018). *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*. Roma: Aracne editrice.

Paolucci, F. (2021). 'Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?', in *MediaLaws* 1: 204–217.

Pariser, E. (2021). *The filter bubble. What the Internet is hiding from you*. New York: Penguin Books.

Peluso, M.G. (2022). 'Intelligenza Artificiale e dati di qualità: la tecnologia come valido alleato', in *MediaLaws* 2: 322-337.

Perego, B. (2022). 'Predictive policing: trasparenza degli algoritmi, impatto sulla privacy e risvolti discriminatori', in *BioLaw Journal - Rivista di Biodiritto* 2: 447-465.

Perri, P. (2020). *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*. Milano: Giuffrè Francis Lefebvre.

Perry, W.L., McInnis, B., Price, C.C., Smith, S., e Hollywood, J.S. (2013). *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations. Rand Corporation*. Santa Monica: RAND Corporation.

Pietrocarlo, E. (2023). 'Predictive Policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali, in *Sistema Penale*: 1-65.

Pietrocarlo, E. (2024). 'La predictive policing nel regolamento europeo sull'intelligenza artificiale', in *La legislazione penale*: 1–35.

Pin, A. (2021). 'Diritti costituzionali e intelligenza artificiale' in P. Moro (a cura di), *Etica, diritto e tecnologia: percorsi dell'informatica giuridica contemporanea*, 45-61. Milano: Franco Angeli.

Polidoro, D. (2020). 'Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale', in *Archivio Penale* 3: 1-41.

Razac, O. (2012). 'La sorveglianza elettronica: l'utopia panoptica rinnovata', in *Materiali foucaultiani* I, 1: 151–168.

Richardson, R., Schultz, J.M., e Crawford, K. (2019). 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice', in *New York University Law Review* 94: 15-55.

Rodotà, S. (2004). *Tecnopolitica: la democrazia e le nuove tecnologie della comunicazione*. Roma: Laterza.

Rodotà, S. (2005). *Intervista su privacy e libertà*. Roma: Laterza.

Rodotà, S. (2014). *Il mondo nella rete. Quali i diritti, quali i vincoli*. Roma: Laterza.

Rodotà, S. (2018). *La vita e le regole*. Milano: Feltrinelli.

Santaniello, M. (2019). 'Il giudizio di Talos. Valutazioni, algoritmi, macchine', in *Rivista di sociologia e scienze umane* IV, 8: 85–102.

Sarra, C. (2022a). *Il mondo-dato: saggio su datificazione e diritto*. Padova: CLEUP.

Sarra, C. (2022b). 'L'uso di dati biometrici nelle procedure di reclutamento al lavoro mediante strumenti di Intelligenza Artificiale. Difficoltà normative multilivello', in *Journal of Ethics and Legal Technologies* 4, 2: 27-49.

Silverman, E. (2023). 'AI and the Administration of Justice in the United States of America', in *Revue Internationale de Droit Pénal*: 5-77.

Snowden, E. (2019). *Errore di sistema*. Milano: Longanesi.

Sofsky, W. (2010). *In difesa del privato*. Torino: Einaudi.

Sunstein, C.R. (2017). *#republic. La democrazia nell'epoca dei social media*. Bologna: Il Mulino.

Surace, M. (2005). 'Analisi socio-giuridica del rapporto tra sorveglianza e diritto alla riservatezza nell'era di Internet', in *ADIR-L'altro diritto*.

Tulumello, S. (2013). 'Panopticon sud-europeo: (Video)sorveglianza, spazio pubblico e politiche urbane' in *Archivio di studi urbani e regionali* 107, 30-51. Milano: Franco Angeli.

Varoufakis, Y. (2023). *Tecnofeudalesimo: cosa ha ucciso il capitalismo*. Milano: La nave di Teseo.

Velo Dalbrenta, D. (2017). 'Crimini predicibili? L'eclissi del diritto penale moderno in Minority Report di Steven Spielberg', in *L'Ircocervo* 2: 40–69.

Willis, J.J., Mastrofski, S.D., e Weisburd, D. (2007). 'Making Sense of COMPSTAT. A Theory-Based Analysis of Organizational Change in Three Police Departments', in Law & Society Review 41, 1: 147-188.

Ziccardi, G. (2022). *Diritti digitali. Informatica giuridica per le nuove professioni*. Milano: Raffaello Cortina Editore.

Zuboff, S. (2019). *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*. Roma: Luiss University Press.

Zuccarini, M. (2009). 'Sotto protezione: sicurezza e sorveglianza nelle politiche europee' in D. Calenda e C. Fonio (a cura di), *Sorveglianza e società*, 83-100. Acireale-Roma: Bonanno Editore.