Giulia Fabini

IL CONTROLLO DATA-DRIVEN: LA NATURA TECNOSOCIALE DELLA (CYBER)SICUREZZA

Bologna
University Press

Giulia Fabini

IL CONTROLLO DATA-DRIVEN: LA NATURA TECNOSOCIALE DELLA (CYBER)SICUREZZA

Bologna
University Press

ll volume è esito del progetto di ricerca "Ecocyber - Risk management for future cyber-physical ecosystems" nell'ambito dello Spoke 8 del Paternariato esteso SERICS - SEcurity and RIghts in the CyberSpace. Finanziato dall'Unione Europea - NextGenerationEU attraverso il Ministero dell'Università e della Ricerca italiano nell'ambito del PNRR – Missione 4 Componente 2, Investimento 1.3 "Partenariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca", Avviso MUR n. 341 del 15/03/2022, Progetto SERICS - SEcurity and RIghts in the CyberSpace, Codice proposta: PE00000014, , CUP: J33C22002810001, finanziato con Decreto MUR n. 1556 del 11/10/2022.

I punti di vista e le opinioni espresse sono esclusivamente quelle dell'autrice e non riflettono necessariamente quelle dell'Unione Europea, né può l'Unione Europea essere ritenuta responsabile per esse.

Fondazione Bologna University Press
Via Saragozza 10, 40123 Bologna
tel. (+39) 051 232 882

www.buponline.com
e-mail: info@buponline.com

ISBN 979-12-5477-682-7
ISBN on line 979-12-5477-683-4
DOI 10.30682/9791254776834

In copertina: foto @ev (Unsplash.com)

Progetto grafico: Sara Celia

Prima edizione: dicembre 2025

Sommario

1. Introduzione

Viviamo in una società in cui risulta sempre più difficile, se non impossibile, distinguere nettamente il reale dal virtuale. Non c'è praticamente nulla che accada esclusivamente nel cyberspazio, senza connessioni con la realtà materiale, né alcun evento (o ben poco) nello spazio fisico che non sia in qualche modo influenzato, mediato o collegato a ciò che avviene online.

Le vite quotidiane si svolgono in una dimensione ibrida, dove il confine tra presenza fisica e interazione digitale è sempre più sfumato. Una persona può essere "presente" in una riunione di lavoro senza esserlo nello spazio materiale e quella presenza può avere lo stesso peso, la stessa efficacia e le stesse conseguenze sul piano operativo. Un litigio su una piattaforma online può generare conseguenze sul piano psichico o legale del tutto tangibili, così come un post può generare denunce, licenziamenti, o campagne di odio collettivo. La sfera digitale non è un luogo "altro", ma una dimensione sempre più fusa con il vissuto quotidiano. Anche la costruzione dell'identità personale si realizza in modo continuo tra il reale e il digitale: i profili social non sono semplici rappresentazioni, ma diventano estensioni riconosciute della persona. Si può "esistere" socialmente – per certi versi anche giuridicamente – solo se si è rintracciabili online. Il numero di follower può determinare opportunità lavorative, credibilità, inclusione o esclusione sociale. Eventi apparentemente "digitali", come la cancellazione di un profilo, possono generare effetti sociali molto più incisivi di eventi che accadono nel solo spazio fisico. Il paesaggio urbano stesso si è trasformato in un'interfaccia digitale. I semafori agiscono come sistemi cyberfisici, regolando il flusso del traffico in tempo reale sulla base dei dati rilevati da sensori distribuiti nel territorio, i pannelli pubblicitari cambiano in base ai dati che li alimentano, e i percorsi

che seguiamo sono spesso suggeriti dai nostri navigatori digitali. Questi sistemi fanno parte di quella rete diffusa e invisibile chiamata Internet delle Cose (*Internet of Things*), in cui oggetti quotidiani – semafori, lampioni, veicoli, ma anche frigoriferi, braccialetti o termostati – sono connessi a Internet, comunicano tra loro, raccolgono dati e prendono decisioni autonome o semiautonome[1]. I gesti "fisici" non sono più necessariamente prioritari o più "veri" rispetto a quelli digitali, che ormai occupano una porzione significativa del nostro vissuto relazionale. Anche i corpi non sono più semplicemente presenti nel mondo fisico, ma diventano "corpi connessi", estesi, aumentati o ridotti da dispositivi. I dati biometrici raccolti da smartwatch o smartphone generano rappresentazioni numeriche della salute, del sonno, del movimento, che spesso sostituiscono la percezione diretta del proprio stato fisico. Il corpo stesso viene esperito, valutato e gestito secondo logiche digitali: una notifica di "stress" da un'app può modificare la percezione soggettiva di sé, un messaggio automatico di "buon riposo" può sostituire il rito della buonanotte.

La distinzione classica tra "online" e "offline" perde così ogni rilevanza descrittiva. Ogni attività è, in una certa misura, già entrambe le cose. Una passeggiata in città è anche una generazione di dati GPS, un acquisto in negozio è spesso preceduto da una ricerca online, un incontro casuale può essere documentato in tempo reale. Il confine tra ciò che è fisico e ciò che è digitale diventa così sempre più poroso, più fluido: non esistono più spazi puramente analogici, né azioni puramente virtuali. Ogni gesto, ogni movimento nello spazio urbano, ogni interazione con un oggetto può attivare processi digitali, registrare dati, generare effetti in tempo reale.

Le tecnologie digitali sono centrali nella vita politica e sociale contemporanea, a tal punto che diventa sempre più difficile distinguere le pratiche e l'impatto del "digitale" dal "sociale" e viceversa. Oggi siamo sempre più "onlife", espressione coniata dal filosofo Luciano Floridi[2] per indicare il venir meno di una distinzione netta e dicotomica tra reale e virtuale, nonché il confondersi di umano, macchina e natura, in una società metaforicamente detta "delle mangrovie". Le mangrovie sono piante che nascono laddove le acque salate del mare e quelle dolci dei fiumi e della pioggia si incontrano, ed è una metafora utile per chiarire cosa si intende qui: la società delle mangrovie è una società in cui l'esperienza quotidiana è il prodotto di una costante mescolanza, di per sé in-

[1] S. Milivojevic, *Crime and Punishment in the Future Internet: Digital Frontier Technologies and Criminology in the Twenty-First Century*, Abingdon, New York, Routledge, 2021.

[2] L. Floridi, *The onlife manifesto: Being human in a hyperconnected era*, Springer International Publishing, 2015.

scindibile, tra online e offline (onlife), e in cui gli spazi sono sempre sia digitali che analogici (infosfera)[3].

Nelle società digitali contemporanee, i meccanismi di controllo sociale e di prevenzione del crimine si fondano sempre più sull'impiego di strumenti tecnologici e, in particolare, sull'uso sistematico dei dati. La raccolta, l'elaborazione e l'analisi delle informazioni costituiscono oggi l'ossatura delle strategie orientate ad anticipare i comportamenti criminali e a garantire l'applicazione delle leggi. Questa crescente dipendenza dai dati ha trasformato le informazioni personali in una risorsa cruciale: esse devono essere acquisite e utilizzate per finalità di sicurezza, ma, al contempo, necessitano di una rigorosa protezione contro accessi non autorizzati e usi impropri. Da questo duplice imperativo nasce una tensione strutturale per le agenzie del controllo, e specialmente per le forze di polizia: da un lato, esse raccolgono e gestiscono informazioni su individui e gruppi, per finalità di controllo, sorveglianza e indagine; dall'altro, devono proteggere i dati che acquisiscono e conservano. Ma non è finita qui. Infatti, chi utilizza tecnologie data-driven per finalità di controllo, dovrebbe anche garantire che tali pratiche siano proporzionate, giustificate e sottoposte a meccanismi di accountability e trasparenza, di non discriminazione, e che rispettino la privacy. Ovvero, nella società digitale, il controllo data-driven deve reggere la prova della cybersicurezza. Dobbiamo però innanzitutto fare un passo indietro e cercare di definire cosa intendiamo con cybersicurezza.

Definire questo concetto non è affatto un'impresa semplice. A ben pensarci, la parola cybersicurezza, con il suo prefisso *cyber-*, incontra gli stessi problemi che incontrano i concetti di cyberspazio e cybercrime che descriviamo nel primo capitolo: possiamo parlare e ragionare di uno spazio cyber come se fosse uno spazio separato dallo spazio del reale? Possiamo parlare di cybercrime, come se questo tipo di criminalità avvenga solo nello spazio cyber senza legami con il mondo reale, con le persone fisiche? Allo stesso modo, cosa significa cybersicurezza in una società onlife?

La struttura del cyberspazio è composta da tre livelli: il primo è quello fisico, fatto di cavi, router, hub, computer, ecc. Il secondo è quello logico, risultante da software, protocolli di comunicazione e altri protocolli. Ovvero, tutto ciò che serve a fare funzionare le macchine. Il terzo, invece, è quello sociale/semantico, ed è composto da persone/utilizzatori. La sicurezza del cyberspazio deve dunque riguardare tutto: software (codici e programmi), hardware (router e host), e utilizzatori degli stessi (le persone)[4]. Difendere computer e dati significa difen-

---

[3] *Ibid.*

[4] G. D'Angelo, G. Giacomello, *Cybersicurezza. Che cos'è e come funziona*, Bologna, Il Mulino, 2023.

dere anche le persone, intese come coloro che utilizzano e che possiedono quei dati. Qui risulta allora interessante rimandare a un lavoro di Raffaella Brighi e Piergiorgio Chiara, che propongono una riflessione su una definizione estensiva della cybersecurity, che poi è anche la definizione intorno a cui si sta ragionando a livello europeo, in particolare con la Cybersecurity Strategy[5]. Questa, utilizzando un approccio top down, ricorda che elevati livelli di sicurezza informatica servono a salvaguardare non solo il funzionamento dei servizi essenziali alla società e all'economia, ma anche l'integrità fisica dei cittadini[6]: «L'asset da proteggere da abusi e manipolazioni diventa quindi la persona»[7]. E questo si rivela di estrema importanza quando la società su cui dobbiamo ragionare è una società digitale. Infatti, comprendere la cybersicurezza intesa in questa versione estensiva richiede anche di collocarla all'interno del più ampio quadro della società digitale.

Come abbiamo avuto modo di mettere a fuoco con gli esempi in apertura di questa breve introduzione, e come vedremo meglio nel primo capitolo, il termine "società digitale" non si riferisce semplicemente alle attività che si svolgono nel cyberspazio, come se questo costituisse una dimensione indipendente e isolata dallo spazio del reale. Al contrario, le società digitali non sono spazi virtuali isolati, ma sistemi integrati in cui i cambiamenti tecnologici, sociali e strutturali ridefiniscono la vita contemporanea. Come osservato in recenti studi, la nostra esistenza è diventata "tecnosociale", con il cyberspazio che costituisce una componente integrante delle interazioni umane, inseparabile dalla dimensione sociale[8]. Le tecnologie digitali non sostituiscono le relazioni interpersonali, ma sono costantemente plasmate da esse e, a loro volta, contribuiscono a plasmarle. Abitiamo un ambiente in cui dimensioni digitali e fisiche interagiscono continuamente, influenzandosi a vicenda. Questo approccio è centrale per comprendere come i rischi legati alla cybersecurity sorgano ed evolvano all'interno di un quadro tecnosociale.

Le tecnologie svolgono un ruolo cruciale sia nel rendere possibili gli atti criminali, sia nel contrastarli. Le modalità con cui le tecnologie vengono impiegate per prevenire il crimine o reagire alla sua commissione comportano rischi significativi per i diritti dei cittadini tanto quanto la criminalità digitale stessa. Ne sono esempio il diritto alla privacy, il diritto di proprietà sui dati persona-

---

5 R. Brighi, P. G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi*, 2021, 21, pp. 18-42.

6 Ivi, p. 23.

7 Ivi, p. 22.

8 G. Stratton, A. Powell, R. Cameron, *Crime and justice in digital society: Towards a "digital criminology"?*, in *International Journal for Crime, Justice and Social Democracy*, 2017, 6(2), pp. 17-33.

li, i diritti di non discriminazione e persino il diritto a un giusto processo, che possono risultare compromessi. I meccanismi di controllo e le strategie di prevenzione dovrebbero basarsi su un uso sicuro ed etico delle tecnologie, facendo della cybersicurezza, intesa in maniera estensiva, una componente fondamentale di tali processi. La raccolta, la protezione e l'utilizzo dei dati rappresentano una delle sfide centrali della contemporaneità.

Per affrontare queste sfide è essenziale costruire un ponte e favorire il dialogo tra gli studi sulla cybersicurezza e quelli sul controllo e la prevenzione del crimine nelle società digitali. Il dibattito critico su tali strategie – ancora nascente ma radicato nell'ambito della criminologia critica – richiama l'attenzione su ulteriori rischi, in particolare quelli legati al potenziale discriminatorio e alle minacce per la privacy insite nei processi di sorveglianza e, talvolta, di criminalizzazione mediata da strumenti data-driven. Mettere in relazione questi saperi consente una comprensione più articolata dei rischi e delle opportunità che gli sviluppi tecnologici comportano rispetto alla criminalità e al controllo. Da un lato, tali sviluppi aprono nuove prospettive per la prevenzione e il controllo del crimine; dall'altro, espongono individui e comunità a nuove vulnerabilità.

È fondamentale che i sistemi tecnologici e le strategie di prevenzione e controllo del crimine siano sottoposti a scrutinio da prospettive molteplici, rafforzandone la capacità di offrire sicurezza senza sacrificare principi di responsabilità, proporzionalità e rispetto dei diritti di tutti gli individui. In tal modo, la connessione fra questi dibattiti critici diventa un pilastro per la costruzione di società digitali più sicure, giuste ed eque. Tale approccio assicura che i sistemi tecnologici siano rigorosamente esaminati affinché servano realmente allo scopo di migliorare la sicurezza, ma che allo stesso tempo si interroghino su quale tipo di sicurezza vogliamo perseguire. Gli studi critici di criminologia da tempo sottolineano l'importanza di porre al centro delle nostre analisi sul controllo e criminalità una sicurezza che sia *sociale*.

Inquadrando la cybersicurezza in questa prospettiva, il presente lavoro intende contribuire a un discorso più sfumato sulla materia, in particolare da un punto di vista criminologico critico, arricchendo il dibattito sulla cybersicurezza e sottolineandone la rilevanza nelle discussioni sul crimine, sul controllo e sulla prevenzione del crimine nelle società digitali.

Il testo si compone di quattro capitoli seguiti da delle brevi riflessioni conclusive.

Nel primo capitolo, vediamo come le riflessioni sulla natura tecnosociale della società digitale si riflettono sullo studio criminologico e critico del controllo data-driven. Per farlo, esploriamo i limiti di come la criminologia fino a tempi recenti, a parte poche eccezioni, abbia affrontato il tema delle trasformazioni

della criminalità e del controllo, focalizzando la propria attenzione sul cybercrime, mentre a noi sembra più corretto interrogare le trasformazioni della criminalità nella società digitale in costante compresenza di elementi online e offline. Nel secondo capitolo, passiamo ad analizzare i processi di datificazione delle interazioni sociali, spiegando cosa sono i big data, come vengono costruiti e poi, nello specifico, come vengono utilizzati nel campo del controllo e nello studio criminologico, per poi ragionare intorno al loro carattere performativo e ai processi di produzione di sapere che da essi scaturiscono. Nel terzo capitolo, approfondiamo l'uso dei big data e del controllo data-driven da un attore specifico all'interno del campo della giustizia penale, ovvero le forze di polizia. Analizziamo, quindi, la nascita della polizia predittiva, le trasformazioni del suo potere discrezionale in forza della tecnologia digitale tra continuità e discontinuità con il passato, per poi focalizzarci sui rischi connessi all'utilizzo di modelli predittivi di polizia: rischi di discriminazione, violazione della privacy, conseguenze sociali, ingerenza del settore privato e della logica del profitto in un settore pubblico, che riguarda la sicurezza di tutte e tutti. Infine, nel quarto capitolo, volgiamo lo sguardo ai sistemi di controllo data-driven in uso tra le forze di polizia in Europa e in Italia, riconoscendo in essi delle pratiche sociomateriali. Le riflessioni conclusive ragionano su due dimensioni della sicurezza e dei dati in relazione al controllo: la sicurezza *dei* dati e la sicurezza *dai* dati. La cybersicurezza tende a corrispondere alla prima delle due. Tramite le riflessioni che sviluppiamo in questo libro, radicate nella criminologia critica, vogliamo invece contribuire al dibattito con una riflessione sulla sicurezza *dai* dati.

Questo libro non sarebbe stato possibile senza l'aiuto e il supporto di quante e quanti, in questi anni, mi hanno incoraggiata ad affacciarmi a questo nuovo campo di studi e hanno avuto la pazienza di spiegarmi concetti che, fino a non molto tempo fa, mi erano oscuri. Questo è il bello della ricerca: affacciarsi su spazi nuovi portando con sè il proprio bagaglio di conoscenze (nel mio caso, la sociologia della polizia e la criminologia critica), ma essendo pronte a rinnovarlo e metterlo in discussione, tracciando al contempo nuove traiettorie possibili. Tutto questo non sarebbe stato possibile senza la mia partecipazione al progetto Ecocyber (spoke 8 di Serics) e senza la pazienza, l'incoraggiamento e il supporto di Raffaella Brighi, che ringrazio per i preziosi consigli, i succulenti pranzetti e le tante opportunità di incontro con chi, in Italia e in Europa, si occupa di questi temi anche da prospettive diverse da quelle con cui sono solita confrontarmi, ma che sicuramente hanno nutrito la spinta a questa interdisciplinarietà di cui tanto si parla e di cui non possiamo fare a meno. Ringrazio anche Piergiorgio Chiara, che ha avuto la generosità e la pazienza di leggere alcune parti di questo

testo e offrirmi le sue sempre ponderate considerazioni. Ringrazio anche il Dipartimento di Scienze Giuridiche dell'Università di Bologna che da anni, prima come assegnista di ricerca, poi come ricercatrice, mi ha accolto, sociologa tra i giuristi e le giuriste, e che oggi è diventata la mia casa. E ovviamente il mio grazie va anche ai colleghi dell'area della sociologia giuridica e della devianza: Alvise Sbraccia, Rossella Selmini, Anna Di Ronco, Stefania Crocitti. In ordine sparso grazie anche ai colleghi cari e alle colleghe care cui mi lega stima e affetto, Dario Melossi, Simone Tuzza, Enrico Gargiulo, Valeria Ferraris, Giuseppe Campesi, Ginevra Sanvitale, con cui mi sono potuta confrontare nei diversi momenti di riflessione e di scrittura di questo lavoro. E poi grazie a Giovi e Marco, che mi hanno lasciato la loro casa per scrivere (corredata di gatti che fanno sempre bene), a Fili che mi ha lasciato la sua camera, a mio padre, che non mi ha mai fatto mancare le verdure dell'orto e a mia madre, che sempre tifa per me. E infine Maurizio, che con la sua cura senza sforzo e la sua presenza forte e attenta mi rende una persona molto fortunata ogni giorno. Va da sé che ogni responsabilità di quanto scritto qui è solo mia.

2. Criminologia critica nella società digitale

2.1 Cybercrime: le fragilità di un concetto

Nelle società digitali, l'evoluzione tecnologica trasforma in profondità le forme della criminalità, i processi attraverso cui essa viene socialmente costruita come tale, le dinamiche di vittimizzazione, nonché i meccanismi di controllo, prevenzione e sorveglianza. In ambito criminologico, tuttavia, l'attenzione rivolta al rapporto tra tecnologia e criminalità si è spesso limitata ad alcune manifestazioni specifiche del cybercrime, quali il cyberbullismo, il cyberstalking, la pedopornografia online e il cyberterrorismo[1]. Nonostante gli sviluppi della riflessione sociologica in ambito di società digitale, la criminologia fatica ancora ad avviare una riflessione teorica sistematica in grado di rispondere alle trasformazioni introdotte dalla tecnologia nel campo della criminalità e del controllo[2].

Con la diffusione delle tecnologie digitali, sono emerse numerose locuzioni per descrivere l'impatto della tecnologia sulla criminalità. Già alcuni decenni fa, termini come *cybercrime* e *computer crime* hanno cominciato a delinearsi come ambiti distinti di studio[3]. C*ybercrime* fa riferimento a reati «in cui l'autore utilizza conoscenze specifiche del cyberspazio», mentre *computer crime* indica reati per commettere i quali «l'autore impiega conoscenze specifiche della tecnolo-

---

1 A. Powel, G. Stratton, R. Cameron, *Digital criminology*, cit.; S. Milivojevic, *Crime and Punishment in the Future Internet*, cit.

2 M. Kaufmann, H. Lomell, *De Gruyter Handbook of Digital Criminology*, Berlin, De Gruyter, 2025.

3 T. Holt, A. Bossler, K. Seigfried-Spellar, *Cybercrime and digital forensics. An Introduction*, Abingdon, New York, Routledge, 2022.

gia informatica [legata ai computer]»[4]. In una prima fase, tale distinzione è utile per specificare in che modo la tecnologia sia incorporata nell'azione criminale[5]. Tuttavia, con la crescente connessione di ogni dispositivo informatico a Internet, tale distinzione è progressivamente venuta meno[6] e oggi i due termini sono spesso utilizzati come sinonimi, tanto nel discorso pubblico quanto in quello accademico.

Un'analisi storica dell'evoluzione dei termini utilizzati per descrivere attività criminali mediate dai computer è proposta da McGuire[7], che esamina le variazioni linguistiche utilizzate tra il 1995 e il 2018. Tra il 1995 e il 2000, erano in uso termini quali *e-crime*[8], *online crime*[9], *digital crime*[10], *net-crime*[11], *technocrime*[12], *internet crime*[13] e *hi-tech crime*[14]. In quel periodo, però, *computer crime* rimaneva il termine dominante. Solo a partire dagli anni 2000 – e con particolare evidenza dopo il 2010 – il termine *cybercrime* ha progressivamente sostituito *computer crime*, affermandosi come etichetta predominante nella letteratura accademica e nelle politiche pubbliche. Sebbene il termine *computer crime* non sia scomparso, *cybercrime* lo ha ampiamente superato in frequenza d'uso, risultando oggi utilizzato il doppio rispetto all'altro. Al terzo posto, tra i termini concorrenti, si colloca *e-crime*.

Come osserva Wall[15], il termine *cybercrime* si è ormai consolidato nel linguaggio comune e accademico, tanto che «we are stuck with it». Ma qual è il problema concettuale posto dal termine *cybercrime*?

---

4 T. Holt, A. Bossler, K. Seigfried-Spellar, *Cybercrime and digital forensics. An Introduction*, cit., p. 10; S. Furnell, *Cybercrime: Vandalizing the information society*, Addison, Wesley, 2002; D. Wall, *Crime and the internet*, in D. Wall (a cura di), *Crime and the internet*, Abingdon, Routledge, 2001, pp. 1-17.

5 D. Wall, *Cybercrime and the internet*, cit.

6 D. Wall, *Cybercrime: the transformation of crime in the information age*, Polity Press. 2007.

7 M. McGuire, *It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime*, in R. Leukfeldt, T. Holt (a cura di), *The human factor of cybercrime*, New York, Routledge, 2020, p. 3-28.

8 Association of Chief Police Officers of England, Wales and Northern Ireland (ACPO), *E-crime Strategy*, London, ACPO, 2009.

9 T. Holt, *Crime on-line: Correlates, causes, and context*, Durham, Carolina Academic Press, 2013.

10 R. Bryant (a cura di), *Investigating digital crime*, London, Wiley-Blackwell, 2008.

11 D. Mann, M. Sutton, *Netcrime: More change in the organization of thieving*, in *British Journal of Criminology*, 1998, (2), pp. 201-229.

12 S. Leman-Langlois, *Technocrime: Policing and surveillance*, London, Routledge, 2014.

13 Y. Jewkes, M. Yar, *Handbook of internet crime*, Devon, Willan Publishing, 2013.

14 S. Brannigan, *High-tech crimes revealed: Cyberwar stories from the digital front*, New York, NY, Addison-Wesley, 2005.

15 D. Wall, *Cybercrime: the transformation of crime in the information age*, cit.

Secondo McGuire[16], adottare questo termine implica assumere la tecnologia come elemento costitutivo della definizione stessa del crimine. Si tratta di un cambiamento non banale. Tradizionalmente, la criminalità viene classificata in base al tipo di danno arrecato, indipendentemente dagli strumenti utilizzati; al contrario, nel caso di *cybercrime*, l'elemento tecnologico diventa la base stessa della definizione. Ne consegue il rischio che ogni reato che coinvolge una componente tecnologica venga incluso nella categoria *cybercrime*, con il risultato di un'etichetta che finisce per racchiudere fenomeni estremamente eterogenei. E anche se esistono reati definiti in base allo strumento impiegato (come i reati con arma da fuoco, con coltello o con veicolo), si tratta di categorie circoscritte e specifiche. *Cybercrime*, invece, rischia di diventare una categoria onnicomprensiva, nella quale può rientrare qualsiasi comportamento deviante che implichi l'uso della tecnologia.

Il dibattito sulla definizione di *cybercrime* è articolato e tutt'altro che risolto. Sono state utilizzate svariate formule per definirlo: «un comportamento dannoso che in qualche modo è legato a un computer»[17]; oppure «un atto criminale che è mediato da un computer»[18]; o anche «un atto criminale che è facilitato o commesso utilizzando un computer»[19]. Per McGuire, elaborare una definizione di *cybercrime* resta indispensabile nonostante le difficoltà, e la questione è tutt'altro che accademica, giacché serve soprattutto per orientare adeguatamente le risposte istituzionali all'evoluzione della criminalità.

In primo luogo, benché si affermi che il *cybercrime* sia in continua ascesa e destinato a diventare la forma di criminalità più diffusa, secondo McGuire tali affermazioni risultano poco credibili:

> L'assenza di precisione nelle concettualizzazioni di cybercrime – e quindi nella sua misurazione – pone dei dubbi riguardo la credibilità di queste affermazioni: in quale periodo il cybercrime può considerarsi la forma più prevalente di criminalità? A quale velocità sta crescendo? E come possiamo avere la sicurezza che i dati scelti sono quelli più appropriati per una particolare definizione/concettualizzazione di cybercrime?[20]

---

16 M. McGuire, *It ain't what it is, it's the way that they do it?*, cit.

17 D. Wall, *Cybercrime and the internet*, cit., p. 3.

18 D. Thomas, I. Loader, *Cybercrime: law enforcement, security and surveillance in the information age*, London, Routledge, 2000.

19 S. Gordon, R. Ford, *On the definition and classification of cybercrime*, in *Journal in Computer Virology*, 2006, p. 15.

20 M. McGuire, *It ain't what it is, it's the way that they do it?*, cit., pp. 27-28.

In secondo luogo, la stessa incertezza si riflette nella possibilità di stimare effettivamente i costi del *cybercrime*. Facciamo un esempio: la vendita online di prodotti contraffatti deve essere inclusa nella definizione di cybercrime oppure no, considerando che escluderla riduce notevolmente la stima complessiva dei costi e, potenzialmente, anche la risposta istituzionale?

Il terzo fronte critico individuato da McGuire riguarda la risposta giuridica al *cybercrime*. Come già evidenziato da Wall[21], non esiste una definizione giuridica univoca di *cybercrime* in nessuna giurisdizione. Se si adottasse come criterio definitorio il tipo di danno prodotto attraverso l'uso del computer, bisognerebbe includere nella definizione di cybercrime una vasta gamma di comportamenti che, per ora, non vi rientrano, tra cui ad esempio la dipendenza dal gioco online. Includere tali fenomeni nella definizione di *cybercrime* avrebbe un impatto rilevante sulla percezione sociale del problema e, dunque, sull'elaborazione delle politiche di intervento anche dal punto di vista del diritto.

Infine, la definizione adottata ha implicazioni rilevanti anche rispetto all'inclusione o esclusione di specifici soggetti come potenziali vittime o autori e autrici di reato. Ad esempio, se si accetta l'idea che il *cybercrime* sia un atto commesso tramite l'uso improprio del computer da parte di individui o gruppi, si esclude a priori la possibilità che uno Stato-nazione possa esserne autore. Questo mostra quanto il concetto di *cybercrime* resti tuttora opaco, ambiguo e spesso investito di un valore simbolico che rimanda più a una costruzione sociale del pericolo che a una categoria analitica stabile.

Sul piano critico, Kevin F. Steinmetz[22] contesta il valore analitico del prefisso *cyber*, definendolo «inutilmente politico, sensazionalista e non chiaro»[23]. Secondo Steinmetz, in origine, il prefisso *cyber-* veniva applicato indiscriminatamente a qualsiasi attività svolta tramite computer (es. *cybershopping*, *cybersex*), mentre oggi è impiegato quasi esclusivamente per descrivere condotte illecite (*cyberbullismo*, *cyberterrorismo*, *cyberguerra*). Tuttavia, il termine offrirebbe scarsa chiarezza concettuale e richiamerebbe una narrazione politica fondata sulla paura e sull'allarmismo.

Nel tempo, sono stati proposti anche altri termini per descrivere il rapporto tra tecnologia e criminalità, come *e-crime*, *technocrime* o *net-crime*. Tuttavia, nessuno di questi riesce a cogliere pienamente la complessità del fenomeno.

---

21 D. Wall, *Cybercrime and the internet*, cit.

22 K. F. Steinmetz, *Against Cybercrime. Towards a Realist Criminology of Computer Crimes*, Abingdon, Routledge, 2024.

23 *Ibid*., p. 13.

In un lavoro precedente, Steinmetz[24] aveva introdotto anche il concetto di *informatized crime*, ispirandosi a Zuboff[25], per indicare una criminalità che prende forma attraverso i processi di mediatizzazione tecnologica. In questo contesto, il crimine è inteso come attività che viene trasformata dalla capacità delle macchine di convertire azioni fisiche in dati e informazioni. Le tecnologie dell'informazione, infatti, svolgono compiti traducendo le azioni fisiche in flussi di dati, e ciò richiede – secondo Zuboff – un insieme di competenze.

Forse il punto è che una definizione di cybercrime rischia di essere fluida e contingente, proprio perché legata a un oggetto (la tecnologia) che muta continuamente. Ovvero, posto che la tecnologia, evolvendosi nel tempo, ha inevitabilmente trasformato anche il cybercrime, una definizione di cybercrime che si fondi su un elemento – la tecnologia – in costante mutamento, non può davvero offrire una base solida per la riflessione teorica e la ricerca empirica su questa tematica. Inoltre, «le tecnologie su cui si basa il cybercrime diventano così radicate nella vita quotidiana che distinzioni significative tra 'crime' e 'cybercrime' non sono più sostenibili»[26].

Nel contesto di una realtà tecnosociale – una società digitale o onlife – risulta infatti sempre più difficile tracciare un confine netto tra crime e cybercrime. La criminalità "priva" di tecnologia sembra destinata a diventare un'eccezione, così come appare altrettanto insostenibile escludere l'intenzionalità umana nella commissione di reati facilitati dall'infrastruttura digitale. Questo solleva una questione teorica centrale: dove si colloca l'agency nella dinamica del cybercrime? La responsabilità della commissione di un cybercrime deve essere attribuita all'umano, alla tecnologia o a un'interazione tra i due? Se si assume che il cybercrime esista perché esiste la tecnologia, occorre anche stabilire in che misura la tecnologia contribuisca attivamente all'evento criminoso.

In questo senso, sono stati proposti diversi tentativi di classificazione della cybercriminalità in base al ruolo svolto dalla tecnologia nello svilupparsi dell'azione criminale.

Un primo tentativo classificatorio di cybercrime partendo dal ruolo svolto dalla tecnologia nell'azione criminale è quello elaborato da Carter[27], che identifica quattro categorie di cybercriminalità:

---

24 K.F. Steinmetz, *Against Cybercrime*, cit.

25 S. Zuboff, *In the age of the smart machine: The future of work and power*, New York, Basic Books, 1988.

26 M. McGuire, *It ain't what it is, it's the way that they do it?*, cit., pp. 35-36.

27 D.L. Carter, *Computer crime categories: How techno-criminals operate*, in *FBI Law Enforcement Bulletin*, 1995, 7, pp. 21-27.

- *Computer as a target*: il computer è l'obiettivo del reato, come nei casi di sabotaggio informatico o furto di proprietà intellettuale.
- *Computer as an instrument*: il computer è lo strumento usato per commettere il reato, come nella frode con carte di credito.
- *Computer as incidental*: il computer è usato marginalmente, senza essere essenziale, come nel caso in cui un membro di una gang lo utilizzi per memorizzare dati o effettuare calcoli (cosa che potrebbe fare anche senza computer).
- *Computer as vehicle for recently invented crimes*: la tecnologia è ciò che viene rubato, come nel caso del furto di software.

Tuttavia, resta forte l'ambiguità su cosa facciano esattamente i computer all'interno del cybercrime, e come questo ruolo debba essere concettualizzato. Alcuni autori parlano di *computer-focused crimes*[28] o di reati commessi dal computer[29]. Altri distinguono tra *involvement*, *assistance* e *relation* della tecnologia nella criminalità cyber.

Un secondo tentativo classificatorio di cybercrime partendo dal ruolo svolto dalla tecnologia è quello di David Wall[30]. La classificazione di Wall, estremamente influente, utilizza un approccio chiamato *per sottrazione.* Infatti, la classificazione nasce dal chiedersi cosa rimarrebbe della criminalità se Internet venisse rimosso dall'equazione.

Da questa domanda derivano tre categorie di criminalità in relazione alla tecnologia:

- *Crimini tradizionali assistiti da Internet*: se Internet venisse meno, il comportamento criminoso continuerebbe attraverso altri mezzi.
- *Cybercrime ibridi*: crimini tradizionali ampliati dall'uso di Internet (come frodi, truffe, pornografia), che esisterebbero comunque, ma con portata più limitata.
- *Cybercrime puri*: reati che possono esistere solo nel cyberspazio, come il furto di identità digitale o gli attacchi DDoS.

Sebbene utile, McGuire ha criticato questa classificazione per due motivi principali: in primo luogo, perché separa rigidamente cyberspazio e spazio fisico,

---

[28] S.M. Furnell, *The problem of categorising cybercrime and cybercriminals*, 2nd Australian Information Warfare and Security Conference, Perth, Australia, 2001.

[29] S. Gordon, R. Ford, *On the definition and classification of cybercrime*, in *Journal in Computer Virology*, 2006, pp. 13-20.

[30] D.S. Wall, *Digital realism and the governance of spam as cybercrime*, in *European Journal on Criminal Policy and Research*, 2005, 10, 4, pp. 309-335.

ignorando la loro integrazione nella realtà digitale contemporanea; in secondo luogo, perché assume l'esistenza di cybercrime "puri", trascurando l'idea di un assemblaggio uomo-macchina in cui tecnologia e intenzionalità criminale sono strettamente intrecciate. Partendo da queste critiche, McGuire – insieme a Dowling – ha quindi rivisitato la classificazione di Wall e ha proposto la cosiddetta definizione tripartita:

- *Cyber-dependent crime*: reati che dipendono completamente dalla tecnologia e che non potrebbero esistere senza di essa, come la creazione e diffusione di malware o gli attacchi DDoS.
- *Cyber-enabled crime*: reati tradizionali che possono essere amplificati dalla tecnologia, come le frodi online o il phishing, ma che esisterebbero comunque anche senza Internet.
- *Cyber-assisted crime*: reati in cui la tecnologia gioca un ruolo marginale, ad esempio nella memorizzazione di dati o nella comunicazione criminale.

Secondo questa classificazione, solo le prime due categorie vengono generalmente considerate come cybercrime in senso proprio. Tuttavia, anche questa definizione non è esente da critiche, poiché lascia irrisolta la questione fondamentale: qual è il ruolo causale della tecnologia nella produzione del crimine? Uno dei principali limiti della distinzione tra *cyber-enabled* e *cyber-dependent crimes* è che essa si fonda unicamente sul ruolo della tecnologia come strumento, senza affrontare la natura criminosa dell'atto in sé[31]. In altre parole, ciò che resta poco definito è cosa renda il cybercrime un crimine: non viene chiarito il contenuto sostanziale della devianza o dell'offesa, ma solo il mezzo attraverso cui essa si manifesta.

Proprio per superare questa carenza, sono stati proposti modelli classificatori alternativi che non si basano esclusivamente sul grado di coinvolgimento della tecnologia, ma piuttosto sul tipo di azione compiuta (*action-based*), sul contesto situazionale o ambientale in cui il reato avviene, o sulle caratteristiche degli attori coinvolti – vittime o autori/autrici. Tali approcci permettono di cogliere più compiutamente l'intreccio tra l'agency dell'umano e della macchina.

Ad esempio, sempre Wall[32] propone una distinzione articolata tra diverse categorie di cybercrime basata sulla natura delle azioni criminose compiute:

---

[31] S. Furnell, *The evolving landscape of technology-dependent crime*, in M.R. McGuire, T. Holt (a cura di), *The handbook of technology, crime and justice*, Abingdon, Routledge, 2017.

[32] D. Wall, *Cybercrime and the internet*, cit.

- *Cyber-trespass*: reati che comportano una violazione di confini digitali (e non fisici), come l'hacking o l'accesso non autorizzato a dati e sistemi.
- *Cyber-deception and theft*: include reati come la frode online e il furto di proprietà intellettuale e la pirateria online.
- *Cyber-porn and obscenity*: comprende non solo reati legati alla pornografia infantile, ma anche comportamenti sessuali online che, pur essendo socialmente stigmatizzati, non sono necessariamente criminalizzati (es. distribuzione di pornografia).
- *Cyber-violenc*e: fa riferimento a forme di violenza emotiva o psicologica esercitate online, come il cyberbullismo o le molestie, ma può includere anche forme più gravi come il cyberterrorismo.

A ben vedere, la prima categoria di Wall è anche sovrapponibile alla categoria di "*computer focused act*", comune nella ricerca cyber, mentre le altre tre appartengono tutte alla categoria degli atti "*computer-assisted*"[33].

La classificazione basata sul tipo di reato non è l'unica possibile. Sono state elaborate ulteriori tipologie classificatorie evidenziando dimensioni diverse del fenomeno. Una si concentra sulle vittime e distingue i cybercrime in base al target dell'attacco: individui, proprietà o Stati[34]. Un'altra tipologia riguarda gli autori di reati, organizzando i reati in base ai profili e alle motivazioni degli autori: hacker, phreaker, mercenari, trafficanti di informazioni, terroristi, estremisti o devianti[35]. Un'ulteriore classificazione è fondata sul tipo di offesa e suddivide i cybercrime in categorie come cyberviolenza, cibercommercio illecito (*cyber-peddling*), accesso non autorizzato e *cyber-squatting*[36]. Queste tassonomie riflettono la complessità e la molteplicità delle forme che il cybercrime può assumere e rappresentano tentativi importanti di mappare un fenomeno in continua evoluzione.

Un'altra proposta rilevante è quella contenuta nella Convenzione del Consiglio d'Europa sul Cybercrime[37], che rappresenta – almeno fino al 2020 – l'unico trattato internazionale largamente riconosciuto in materia. Essa identifica cinque aree principali:

---

33 G. Stratton, A. Powell, R. Cameron, *Crime and justice in digital society: Towards a 'digital criminology'?*, in *International Journal for Crime, Justice and Social Democracy*, 2017, 6, 2, pp. 17-33.

34 S. Ghernauti, *Cyber Power: crime, conflict and security in cyber space*, EFPL Pess, CRC Press, 2013.

35 D. Thomas, I. Loader, *Cybercrime,* cit.

36 H.S. Brar, G. Kumar, *Cybercrimes: A Proposed Taxonomy and Challenges*, in *Journal of Computer Networks and Communications*, 2018, pp. 1-18.

37 Council of Europe, *Convention on cybercrime*, European Treaty Series, No. 185, 2001.

- Reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici (es. accesso illegale, intercettazione illecita, interferenze su dati o sistemi, uso improprio di dispositivi).
- Reati informatici in senso stretto (es. falsificazione e frode commesse tramite computer).
- Reati legati ai contenuti (es. pornografia infantile).
- Violazioni della proprietà intellettuale.
- Responsabilità accessorie (es. tentativi, complicità, o istigazione al reato).

Secondo McGuire[38], definire il cybercrime a partire dalle categorie legali – cioè dai reati riconosciuti – ha il vantaggio di mantenere il discorso ancorato a un terreno normativo e operativo, evitando derive teoriche troppo astratte. Questa impostazione si è dimostrata particolarmente utile nella fase iniziale dello studio sul cybercrime, per identificare in modo concreto le tipologie di condotte illecite emergenti. Tuttavia, col tempo, tale approccio ha mostrato limiti evidenti: ciò che è considerato reato varia notevolmente tra giurisdizioni, culture e momenti storici.

Esiste anche una linea di classificazione basata sullo *spazio* in cui si verifica il reato. In questo senso, il *cybercrime* è stato interpretato come *Cyberspace crime*[39]. Tale prospettiva invita a interrogarsi su cosa cambi, in termini di criminalità e di controllo, quando l'atto deviante si colloca all'interno di uno spazio digitale. Tuttavia, anche in passato sono emersi nuovi spazi – come il telefono o il telegrafo – che hanno trasformato il contesto dell'attività criminale, senza per questo produrre intere nuove categorie di reati[40].

Alcuni autori[41] hanno cercato di esplorare approcci spaziali alternativi, capaci di riconoscere come la tecnologia digitale estenda le opportunità criminali, pur mantenendo al centro l'agency umana. La tecnologia, infatti, non agisce mai in isolamento, ma sempre in relazione a soggetti umani che ne sfruttano le potenzialità. La distinzione tra cyberspazio e spazio fisico, così come quella tra agency tecnologica e agency umana, appare sempre più problematica in una società digitale profondamente integrata.

---

38 M. McGuire, *It ain't what it is, it's the way that they do it?*, cit.

39 D.S. Wall (a cura di), *Cyberspace crime*, London, Routledge, 2003.

40 M. McGuire, *It ain't what it is, it's the way that they do it?*, cit.

41 M. Yar, *Cybercrime and society*, London, Sage, 2006; M.R. McGuire, *Hypercrime: The new geometry of harm*, London, Routledge, 2008; K. Jaishankar, *Space transition theory of cyber crimes*, in F. Schmallager, M. Pittaro (a cura di), *Crimes of the internet*, Upper Saddle River, NJ, Prentice Hall, pp. 283-301.

McGuire[42] riprende questa prospettiva, osservando che ciò a cui assistiamo è una fitta interconnessione tra corpo e tecnologia: le tecnologie dell'informazione e della comunicazione (ICT) non solo estendono l'agency umana nello spazio (ad esempio permettendo di agire a distanza), ma l'amplificano anche in termini di forza, rapidità e accessibilità. Questo potenziamento è reso possibile dall'esplosione della connettività digitale, che genera uno stato di *iperconnessione* in cui, come scriveva McLuhan già nel 1967[43], si è «connessi a tutti, ovunque e in qualsiasi momento». Questa iperconnessione non genera semplicemente un *cyberspazio*, ma un vero e proprio *iperspazio*, che dà origine a nuove possibilità relazionali, sociali e criminogene[44]. In questo contesto, il cybercrime può essere ripensato come *hypercrime*: non un reato immateriale o misteriosamente digitale, ma una forma concreta di devianza resa possibile dall'ampliamento dell'agency umana attraverso la tecnologia. Ciò che cambia è il modo in cui le capacità criminali vengono potenziate, estese, accelerate.

Una simile concezione riconduce il crimine digitale a una rete di connessioni fisiche, sociali e psicologiche potenziate dalle ICT. In tal modo, il cybercrime può essere interpretato non solo come reato *nel* digitale, ma *del* digitale: espressione di un nuovo regime di interazione, possibilità e responsabilità.

Alla luce di queste trasformazioni – spaziali, tecnologiche e concettuali – appare evidente che le tradizionali categorie criminologiche faticano a restituire la complessità dei fenomeni devianti nell'ambiente digitale. L'iperconnessione, la compenetrazione tra umano e tecnologia, e la natura sempre più ibrida dello spazio sociale richiedono un ripensamento non solo delle classificazioni del crimine, ma anche degli strumenti teorici e metodologici della disciplina. È proprio da queste premesse che nasce la cosiddetta criminologia digitale, un campo emergente che si propone di interrogare la criminologia stessa di fronte alle sfide poste dalla società digitale. Prima di passare alla trattazione del campo della criminologia digitale, soffermiamoci un attimo nel concetto di società digitale, da cui la criminologia digitale, per l'appunto, si sviluppa.

---

42 M. McGuire, *It ain't what it is, it's the way that they do it?*, cit.

43 M. McLuhan, Q. Fiore, *The medium is the massage: An inventory of effects*, San Francisco, CA, Hardwired, 1967.

44 A. Quan-Haase, B. Wellman, *Hyperconnected net work: Computer-mediated community in a high-tech organization*, in C. Heckscher, P. Adler (a cura di), *The firm as a collaborative community: Reconstructing trust in the knowledge economy*, New York, NY, Oxford University Press, 2006 pp. 281-333; T. Friedman, *It's a 401(k) world*, in *The New York Times*, 2013, May 1; C. Vitale, *Networkologies: A philosophy of networks for a hyperconnected age*, Alresford, UK, Zero Books, 2014.

2.2 La natura sociale della tecnologia

A lungo si è parlato di cyberspazio come di una dimensione separata dalla realtà fisica, uno spazio virtuale in cui le cose accadono parallelamente al loro accadere nella realtà fisica. Sin dall'inizio degli anni Novanta, il termine *cyberspace* ha fatto il suo ingresso nella cultura popolare attraverso la fantascienza e le arti. Esso era inteso come il quinto dominio di potere dopo terra, aria, oceani e spazio, l'unico artificiale[45].

Definire cosa sia il cyberspazio è stata ed è tuttora un'impresa scientifica di non poco conto. Ne esistono numerose definizioni.

David D. Clark definisce il *cyberspace* come «la collezione di dispositivi informatici connessi da reti, in cui le informazioni elettroniche sono archiviate e utilizzate, e dove avviene la comunicazione»[46]. Il cyberspace ha lo scopo di «processare, manipolare e sfruttare le informazioni, facilitare e aumentare la comunicazione tra le persone, e supportare l'interazione tra persone e informazioni»[47]. Clark non elabora una vera e propria definizione di che cosa sia il cyberspazio, ma lo descrive fornendo un catalogo delle sue caratteristiche. Il suo modello si sviluppa su quattro livelli: persone, informazione, logica, fisico. Ogni livello rappresenta una dimensione fondamentale della realtà digitale. Considerare il cyberspace come l'insieme di questi quattro livelli consente non solo di comprenderne la complessità tecnica, ma anche di interrogarsi sulle dinamiche di potere e controllo che si manifestano in ciascun ambito.

Il primo livello, denominato fisico, costituisce la base materiale del cyberspazio. Esso include i dispositivi informatici – come server, router, sensori e infrastrutture di rete – attraverso i quali avviene la connessione e il trasporto dei dati. Clark sottolinea che, sebbene questo livello sia apparentemente il più semplice da comprendere, poiché tangibile e geograficamente situato, esso rappresenta anche un punto critico per l'esercizio del controllo. Il possesso e la gestione delle infrastrutture fisiche determinano, infatti, chi ha accesso alla rete e a quali condizioni, rendendo visibili le implicazioni geopolitiche e giurisdizionali del cyberspazio. Il secondo livello, definito logico, riguarda le strutture astratte e i protocolli che regolano il funzionamento delle reti. Si tratta del livello in cui si definiscono le logiche dell'interconnessione, attraverso standard e servizi che permettono la costruzione di applicazioni sempre più complesse. Secondo

---

[45] M. Mayer, F. Gabrielli, *Next generation Eu: The digital transition's policy dilemmas*, in *Rivista di Digital Politics*, 2022, 3, pp. 1-22.

[46] D.D. Clark, *Characterizing cyberspace: Past, present and future*, ECIR Working Paper, 2010, 3, MIT Political Science Department.

[47] *Ibidem*.

Clark, è in questa dimensione che si prendono le decisioni fondamentali sul disegno della rete, che influenzano direttamente la sua apertura, flessibilità e vulnerabilità. Il potere, in questo contesto, risiede nella capacità di progettare e controllare le architetture logiche, modellando le possibilità di azione degli utenti e degli sviluppatori. Il terzo livello, quello informativo, è dedicato alla creazione, gestione e distribuzione dei contenuti digitali. Qui si situano i dati – statici o dinamici – che costituiscono l'esperienza del cyberspazio per l'utente finale: testi, immagini, video, documenti e metadati. Clark osserva come, nel tempo, il carattere dell'informazione in rete sia mutato, passando da una struttura statica a una generativa e personalizzata. Le questioni di autenticità, proprietà, veridicità e accessibilità dell'informazione diventano quindi centrali, così come i meccanismi di controllo, censura e manipolazione che possono essere esercitati da chi possiede o gestisce tali contenuti. Infine, il livello più alto del modello è quello delle persone. Gli individui non sono soltanto fruitori passivi del cyberspazio, ma ne sono co-costruttori attivi. Essi interagiscono, creano contenuti, plasmano piattaforme e contribuiscono all'evoluzione della rete stessa. In questo contesto, il potere si manifesta nella capacità di influenzare comportamenti, di gestire identità digitali e di orientare dinamiche sociali e culturali. L'adozione diffusa di strumenti di comunicazione digitale sta generando nuove forme di partecipazione, ma anche nuove vulnerabilità, soprattutto in relazione alla sorveglianza e alla manipolazione psicologica. Secondo Clark, nel cyberspazio, le dinamiche di potere sono distribuite lungo tutte le sue dimensioni. Ogni livello comporta potenziali punti di controllo che possono essere esercitati da attori diversi – governi, imprese, sviluppatori, utenti – rendendolo uno spazio fluido e conteso, tanto sul piano tecnico quanto su quello politico e sociale.

Ci si è tuttavia presto resi conto dei limiti insiti nel concetto stesso di cyberspazio come sfera separata dalla realtà fisica e sociale, come termine utilizzato per fare riferimento esclusivo agli aspetti informatici e di rete (es. comunicazioni digitali, infrastrutture informatiche, cyberattacchi). A un certo punto, è apparso evidente quanto le dinamiche digitali producano effetti concreti sul mondo reale, e quanto sia inadeguato pensare al digitale come a una dimensione isolata o autonoma rispetto alla sfera materiale e relazionale. Del resto, già dalle riflessioni sulle dinamiche di potere e realtà digitale di Clark è chiaro che la dimensione del digitale sia influenza dal reale, e viceversa.

Ben presto, il concetto stesso di cyberspazio si è rivelato non adatto a descrivere l'impatto della rivoluzione digitale su tutti gli aspetti della vita umana. Per questo, oggi, più che di cyberspazio diventa importante parlare di società digitale.

Cosa si intende per 'digitale'?

Secondo la definizione proposta da Heather Horst e Daniel Miller[48], il termine digitale si riferisce a qualsiasi elemento che possa essere sviluppato attraverso la logica binaria del codice 1/0, o ricondotto a essa. Quindi digitale non è sinonimo di computer né tanto meno di codice, ma fa riferimento all'intreccio costante tra tecnologia e sociale. Un intreccio per il quale l'uno non è né può essere separato dall'altro. Il punto è che le tecnologie digitali non esistono al di fuori della realtà sociale, ovvero le tecnologie digitali non sostituiscono l'interazione sociale, non producono relazioni sociali e modi di fare completamente nuovi; più che altro consolidano e spingono modi di fare già emergenti. Contribuiscono a plasmare e a modificare l'organizzazione sociale, mentre vengono modificate e plasmate a loro volta[49].

Similmente, si parla di società digitali ("digital society") per riferirsi all'insieme integrato rappresentato dalle tecnologie digitali e dalla società, ovvero per riferirsi all'insieme dei cambiamenti sociali, tecnologici e strutturali che investono le società contemporanee. Un tutto che è più della somma delle varie parti[50]. La vita politica e sociale contemporanea, i processi culturali, sociali, economici che la caratterizzano hanno una natura "tecnosociale"[51]. Il cyberspazio non si sostituisce all'interazione umana, né esiste separatamente da essa. Digitale e sociale sono costantemente parte l'uno dell'altra e si danno forma reciprocamente.

In sintesi, "digital society" è un concetto più ampio e critico rispetto a cyberspazio e mette in luce le trasformazioni strutturali e culturali prodotte dalla digitalizzazione, andando oltre l'idea tecnica e limitata di quello.

In questo scenario, la tecnologia non può più essere considerata un semplice strumento neutro nelle mani degli individui. Essa si configura come un elemento strutturale della società, una componente organica delle relazioni sociali, economiche, politiche e culturali. La tecnologia digitale non solo media, ma produce significati, organizza il tempo e lo spazio, struttura le interazioni e influenza la costruzione dell'identità individuale e collettiva. Non siamo semplicemente utenti della tecnologia: ne siamo anche soggetti, destinatari e a volte inconsapevoli oggetti. Ogni dispositivo, ogni app, ogni piattaforma, ogni rete sociale è portatrice di un certo modo di vedere il mondo, di rappresentarlo, di normarlo.

---

48 H. Horst, D. Miller, *The digital and the human: A prospectus for digital anthropology*, in H. Horst, D. Miller (a cura di), *Digital Anthropology*, New York, Berg, 2013, p. 5.

49 E. Ruppert, E. Isin, D. Bigo, *Data politics*, in *Big Data & Society*, 2017, 4(2), pp. 1-7; B. Aragona, S. Stefanizzi, *Società digitale: interrogativi, aree di ricerca e ruolo della sociologia*, in *Sociologia Italiana*, 2024, 7, pp. 7-19.

50 A. Powel, G. Stratton, R. Cameron, *Digital criminology. Crime and justice in digital society*, Abingdon, Oxon, Routledge, 2018.

51 Ivi.

La società digitale non è quindi soltanto una società che fa uso di tecnologie informatiche: è un ambiente complesso, un ecosistema socio-tecnico in cui i confini tra umano e artificiale, tra naturale e costruito, sono costantemente messi in discussione. La comunicazione, la memoria, l'organizzazione del lavoro, l'accesso all'informazione, la gestione delle emozioni – tutti questi aspetti dell'esperienza umana sono sempre più modellati da algoritmi, dispositivi e architetture digitali. La tecnologia, lungi dall'essere neutra, è intrinsecamente sociale: è progettata, sviluppata, diffusa e utilizzata all'interno di contesti storici e culturali specifici, da attori con interessi precisi, che riflettono (e spesso amplificano) disuguaglianze esistenti.

La natura sociale della tecnologia si rivela, inoltre, nella sua capacità di configurare nuovi spazi di socializzazione, ma anche di esclusione. Il digitale è, allo stesso tempo, veicolo di accesso e strumento di controllo, generatore di opportunità e meccanismo di sorveglianza. L'accesso alle tecnologie, la possibilità di partecipare pienamente alla società digitale, non è equamente distribuito. Esistono barriere economiche, culturali, infrastrutturali, che riproducono – e in alcuni casi aggravano – le linee di frattura della società analogica: classe, razza, genere, età. Si configura così una nuova forma di disuguaglianza, un *digital divide* che è anche un *social divide*[52].

Il concetto di società digitale è più adatto per analizzare i cambiamenti profondi nelle società contemporanee prodotti dalla transizione digitale. Parlando di società digitale, si fa riferimento a un cambiamento sociale profondo: non ci si riferisce solo a strumenti tecnologici, ma a come essi modificano il comportamento umano, le relazioni sociali, le abitudini quotidiane. Comprende tutte le sfere della società: finanza, commercio, cultura, politica, educazione, diritti civili. Riflette l'interconnessione sistemica tra le nuove tecnologie digitali e gli ambiti militari, economici, istituzionali; le tecnologie digitali non agiscono in isolamento dal resto, ma penetrano in tali ambiti e li trasformano in modo interdipendente. Inoltre, parlando di società digitali, si mira a trovare una maniera per analizzare le sfide democratiche, sociali e geopolitiche della contemporaneità, che hanno per forza di cose a che fare con il digitale, come la sorveglianza, la disinformazione, la sicurezza e, nondimeno, il controllo e la criminalità. Di questo ci si occupa nel prossimo paragrafo.

---

[52] J. Van Dijk, *The Deepening Divide: Inequality in the Information Society*, Thousand Oaks, Sage, 2005; L. Sartori, *Digital Divide. Le nuove disuguaglianze nella società dell'informazione*, Bologna, Il Mulino, 2006.

2.3 Criminologia digitale

Vari studi criminologici hanno messo in luce l'impatto crescente delle tecnologie dell'informazione e della comunicazione sulla giustizia penale e sulla sicurezza: dall'uso di big data e algoritmi predittivi nella polizia, alle nuove forme di criminalità online, fino alle sfide normative e deontologiche legate alla sorveglianza digitale[53]. Tuttavia, è proprio in reazione a questo scenario – in cui la tecnologia è considerata neutrale e oggettiva e in cui la criminalità è indagata soprattutto come cybercriminalità – che prende forma un filone di riflessione diverso, quello della criminologia digitale.

La criminologia digitale emerge dalla necessità di comprendere le trasformazioni della criminalità e del controllo nel contesto di una società digitale e si pone come un avanzamento teorico ed empirico rispetto allo studio del cybercrime. Lascia da parte il dibattito sulle definizioni di cybercrime, poiché la costante compresenza tra realtà online e offline che caratterizza le società digitali rende sempre più difficoltoso distinguere la "cybercriminalità" dalla "criminalità tradizionale": queste due categorie non possono essere mai separate, tanto che si può forse iniziare a parlare di criminalità digitale[54] invece che di cybercrime.

In Italia si è recentemente affermata una riflessione strutturata su questi temi, in particolare intorno alle Università di Trento e Verona. Dal 2021 è attivo presso queste sedi un centro di ricerca dedicato allo studio della criminalità nella società digitale, diretto da Andrea Di Nicola, autore del volume *Criminalità e criminologia nella società digitale*. Il testo ha il merito di sistematizzare, in lingua italiana, il dibattito internazionale sulla cybercriminalità, offrendo al contempo una proposta teorica originale che mira a superare il concetto stesso di cybercrime.

Di Nicola sostiene che lo studio criminologico oggi deve confrontarsi con uno scenario nuovo, in cui le tecnologie fanno parte della vita di tutti giorni e difficilmente ciò che accade nel reale non ha un qualche tipo di legame con il digitale: dunque anche la criminalità si sviluppa e si trasforma in una costante compenetrazione tra sfera online e sfera offline. Propone allora di superare la definizione tradizionale di cybercrime, introducendo il concetto di criminalità digitale e una relativa teoria dello spettro della criminalità (*spectrum theory*). Secondo questa prospettiva, i comportamenti criminali in una società digita-

---

53 Tra gli altri, si vedano, ad esempio: P. Fussey, D. Murray, *Facial Recognition Surveillance: Policing and Human Rights in the Age of Artificial Intelligence*, Oxford, Clarendon Studies in Criminology, 2025. A. Lavorgna, T.J. Holt (eds.), *Researching cybercrimes: methodologies, ethics and critical approaches*, London, Palgrave Macmillan, 2021.

54 A. Di Nicola, *Criminalità e criminologia nella società digitale*, Milano, FrancoAngeli, 2021.

le non possono essere né completamente online né completamente offline. La criminalità tradizionale, oggi, difficilmente rimane avulsa dalla tecnologia. Di Nicola propone di collocare la criminalità lungo un continuum: a un estremo si trovano i reati pienamente tecnologici e virtuali, che non potrebbero esistere senza l'ambiente digitale; all'estremo opposto, crimini puramente fisici, privi di qualsiasi componente tecnologica. Tra questi poli si collocano una molteplicità di fenomeni ibridi, in cui la tecnologia assume un ruolo variabile – talvolta marginale, talvolta centrale – nella dinamica del comportamento criminale. Gli esempi possono essere tanti: la tecnologia viene utilizzata per le comunicazioni legate ad eventuali attività delittuose che poi avvengono offline; il reato si sviluppa nella realtà online (come cyberbullismo, cyberstalking, crimini di odio online, ecc.) ma con ripercussioni decisamente materiali nella vita della vittima; un soggetto elabora e commette un reato interamente nella realtà offline, ma viene ripreso dalle videocamere di sorveglianza, viene identificato con tecnologie di riconoscimento facciale, o viene segnalato alla polizia da un passante tramite app specifiche; vengono utilizzati metodi di tracciamento come il gps del telefono per ricostruire il percorso del reo; a volte, è il reo a utilizzare il gps per geolocalizzare ad esempio il proprietario di un appartamento che intende svaligiare, per essere sicuro che non sia in casa. Dunque, nella proposta di Di Nicola, la nozione di "criminalità digitale" non coincide con quella di cybercrime: mentre quest'ultima tende a identificare specifiche tipologie di reati, la prima intende abbracciare un insieme più ampio e articolato di fenomeni, legati in modo più profondo alla struttura socio-tecnologica della società digitale. Secondo questa impostazione teorica, l'interazione tra esseri umani, macchine e oggetti digitali varia in funzione della posizione lungo lo spettro. Con essa muta anche il peso e il ruolo che la tecnologia ha nella commissione di un reato e quindi anche (forse?) la responsabilità umana nell'atto criminoso e del danno che ne deriva. Un ragionamento di questo tipo può essere utile per riflettere intorno al grande tema dell'*accountability*, importantissimo quando si parla di criminalità (ma anche di controllo) in relazione alle tecnologie.

Un altro fattore cruciale su cui la teoria dello spettro della criminalità ci porta a riflettere è il grado di alfabetizzazione digitale degli attori coinvolti, che incide sia sulla natura dei comportamenti devianti, sia sulle strategie di contrasto messe in atto.

La criminologia digitale emerge all'interno di un contesto caratterizzato da una profonda trasformazione tecnologica delle pratiche sociali, istituzionali e comunicative. La digitalizzazione non ha semplicemente introdotto nuovi strumenti per commettere reati o nuove tecniche per contrastarli, ma ha modificato strutturalmente le modalità attraverso cui il crimine viene definito, interpretato

e governato. È così che in questo terreno emergente della criminologia digitale, è anche presente un orientamento di tipo critico che si propone di andare oltre la mappatura degli strumenti digitali in mano alla criminalità, al controllo, alla sorveglianza e all'investigazione, per interrogarsi sulle forme di potere, esclusione e produzione di soggettività che attraversano gli ambienti digitali e le infrastrutture tecnosociali della contemporaneità. Di Nicola si pone in posizione critica rispetto ad alcune letture più radicali e teoricamente orientate della criminologia digitale – in particolare quella elaborata da Powell, Stratton e Cameron[55] – ritenendole non sufficientemente ancorate all'evidenza empirica. È proprio a queste prospettive critiche, le quali propongono un ripensamento profondo delle categorie criminologiche alla luce delle trasformazioni digitali, che si dedicano le prossime due sezioni.

2.4 L'approccio della criminologia critica

Questo testo adotta un approccio di criminologia critica per leggere le conseguenze della datificazione del controllo e i rischi che tale processo pone ai diritti delle cittadine e dei cittadini (e dei non-cittadini) nelle società digitali.

L'oggetto, l'estensione, la metodologia, le conclusioni teoriche e pratiche della ricerca criminologica variano notevolmente a seconda del modo di concepire il fenomeno criminale. Una prospettiva critica in criminologia invita a considerare il crimine non come un fenomeno naturale, oggettivo o universale, né il criminale semplicemente come colui o colei che commette un atto illecito, né tantomeno il controllo istituzionale come una semplice reazione al reato. Al contrario, la criminologia critica parte dal presupposto che il crimine sia l'esito di un processo di costruzione sociale. Una prospettiva di criminologia critica studia i processi di criminalizzazione, ovvero quei processi politici, storici e culturali, attraversati da relazioni di potere, tramite cui la criminalità viene costruita come fatto sociale. In altre parole, il crimine è, prima di tutto, il risultato di definizioni che identificano determinati atti come criminali. Queste definizioni – in primis di natura giuridica – variano nel tempo e nello spazio: ciò che oggi è considerato reato potrebbe non esserlo domani, e ciò che costituisce un crimine in una giurisdizione potrebbe non costituirlo in un'altra. L'indagine sulla criminalità e sul sistema di controllo diventa quindi una via per indagare le società contemporanee in veloce e continua trasformazione.

[55] A. Powel, G. Stratton, R. Cameron, *Digital criminology*, cit.

La criminologia critica viene elaborata innanzitutto da Ian Taylor, Paul Walton e Jock Young nel famoso *The New criminology: for a social theory of deviance*[56]. L'idea di base è che la criminalità e i processi di criminalizzazione affondino le proprie radici nelle dinamiche di potere che strutturano le società[57]. Utilizzando una prospettiva sociologica, la criminologia critica lascia in secondo piano lo studio delle cause individuali del crimine per aprirsi allo studio di quelle collettive. Non è il livello individuale quello che interessa la criminologia critica. Si può forse affermare che la criminologia critica rifletta sulla società a partire dai modi in cui questa ha scelto di codificare, leggere, gestire e punire la criminalità. La critica è rivolta, dunque, al contesto sociale in cui i processi di criminalizzazione si determinano, producendo e riproducendo relazioni di potere ineguali e gerarchiche.

Come spiega in maniera puntuale Alvise Sbraccia[58], la criminologia critica nasce dall'assemblaggio di due matrici teoriche: le teorie dell'etichettamento e il marxismo.

Le teorie dell'etichettamento, di matrice interazionista[59], si sviluppano negli Stati Uniti negli anni Sessanta. Esse sottolineano che la criminalità, e dunque anche la figura del/della criminale, sono l'esito di un processo di costruzione sociale. Dipendono, in primo luogo, dal «potere di nominazione dell'autorità pubblica», cioè dal potere che l'autorità pubblica ha di nominare le cose, definire cosa è criminalità e cosa non lo è; in secondo luogo, dagli «strumenti di produzione di stigma sociali», ovvero dagli strumenti che l'autorità pubblica utilizza per esercitare controllo sugli atti che ha nominato come criminali. Questi

---

56 I. Taylor, P. Walton, J. Young, *The New Criminology: For a Social Theory of Deviance*, London–New York, Routledge, 1973.

57 P. Walton, J. Young, *The New Criminology Revisited*, in P. Walton, J. Young (a cura di), *The New Criminology Revisited*, London, Palgrave Macmillan, 1998, p. vii.

58 A. Sbraccia, *Criminologie post-coloniale*, in C. Rinaldi, P. Saitta (a cura di), *Criminologie critiche contemporanee*, Milano, Giuffrè Francis Lefebvre, 2018, pp. 27-49.

59 Quando si parla di interazionismo simbolico, si fa in particolare riferimento a Herbert Blumer, il quale tuttavia prende le mosse dalle teorie di Mead. Quest'ultimo ha incentrato la sua indagine intorno alle problematiche connesse alla comunicazione e al linguaggio, che considera fondamentali per ogni alto aspetto dell'organizzazione sociale. Infatti, i membri di un'organizzazione sociale stabiliscono i significati delle cose, sia negli aspetti materiali che immateriali, tramite l'interazione. La maniera in cui i membri di un'organizzazione sociale raggiungono un significato condiviso di un dato oggetto è tramite l'interazione, e il significato è sempre frutto di una mediazione. Tuttavia, e questo è centrale nella prospettiva critica, la relazione entro la quale l'interazione si dà è sempre una relazione di potere: la possibilità di influire sullo stabilire i significati condivisi di un dato oggetto non è la stessa per tutti i membri che partecipano all'interazione. Dunque, esistono relazioni di potere nelle definizioni, nelle etichette e nei significati. Tale aspetto diventa particolarmente rilevante nel contesto della democrazia e del controllo sociale, nel momento in cui ci interroghiamo su chi possiede il potere definitorio circa ciò che ci circonda. D. Melossi, *Stato, controllo, devianza*, Bologna, Il Mulino, 2002.

strumenti sono la messa al bando, il processo, la condanna da parte del giudice, il carcere, in grado per l'appunto di stigmatizzare i soggetti cui esse si rivolgono[60]. Le teorie dell'etichettamento invitano a comprendere i processi di criminalizzazione osservando, a livello micro-sociale, l'interazione tra i soggetti nel corso delle dinamiche di attribuzione di significato e nelle pratiche del controllo.

Nell'ambito delle teorie marxiste, la criminalità e il controllo sono letti attraverso le lenti del conflitto di classe. Ciò significa che il controllo esercitato dal diritto penale è concepito come uno strumento al servizio dell'*élite* politica ed economica, finalizzato a preservare l'ordine sociale funzionale alla riproduzione dei rapporti di potere capitalistici. In questa prospettiva, il diritto penale non rappresenta un meccanismo imparziale di regolazione dei comportamenti criminali, ma agisce selettivamente per tutelare gli interessi delle classi dominanti. L'intervento penale, quindi, non si limita a perseguire tutte le condotte dannose, bensì tende a criminalizzare forme di dissenso e conflitto che minacciano l'equilibrio del sistema produttivo e il controllo sociale esercitato sulle classi subalterne. L'invito, in questo caso, è a ricercare le *grand narrative*, ovvero a porre attenzione alle macro-dinamiche del controllo.

Nella criminologia critica, i due orientamenti – teorie dell'etichettamento e teorie marxiste – si fondono e trovano un minimo comun denominatore nell'attenzione alle pratiche selettive del controllo. Infatti, tra la commissione di un reato e lo scontare una pena in carcere intervengono tutta una serie di passaggi durante i quali agiscono dei meccanismi di filtro: bisogna che un comportamento sia stato definito come criminale; è necessario che tale comportamento criminale sia tra quelli perseguiti; bisogna essere tra i soggetti denunciati per quello specifico comportamento criminale; bisogna arrivare alla condanna; la condanna dovrebbe essere eseguita con una pena detentiva. Focalizzarsi sulle relazioni di potere sottese al diritto e alla sua applicazione (diseguale) è al centro dell'indagine criminologica critica.

La criminologia critica problematizza il fatto che la selettività del sistema penale operi non solo nel senso di colpire in maniera sproporzionata alcuni reati piuttosto che altri, ma anche alcuni segmenti della popolazione piuttosto che altri, tipicamente quelli più marginalizzati. Ma non è finita qui. Infatti, non solo alcuni reati vengono più facilmente selezionati rispetto ad altri e alcune persone sono più facilmente target dell'attenzione degli agenti del controllo: esiste una disparità anche nella risposta della giustizia penale, che sarà più severa nei confronti di taluni soggetti e più clemente nei confronti di altri, anche a parità di reato. Perché ciò avviene? Alcune ricerche hanno sottolineato che questo può

[60] A. Sbraccia, *Criminologie post-coloniale*, cit.

essere dovuto alle differenti condizioni materiali che si ripercuotono nel potersi o meno permettere un avvocato competente o nella difficoltà di usufruire degli arresti domiciliari, o dal fatto che nel processo decisionale tanto i giudici[61] quanto le forze dell'ordine[62] possono essere influenzati da pregiudizi e stereotipi (individuali o strutturali) basati su costruzioni sociali come la "razza", il "genere" o altro.

Verso la metà degli anni Ottanta, nuovi concetti come quelli di razza e genere vanno ad allargare la prospettiva con cui la criminologia critica osserva la criminalità. Razza, genere e classe diventano le linee di potere che, nel loro intersecarsi[63], strutturano l'azione sociale: influiscono sui comportamenti, sulle aspettative rispetto a tali comportamenti, sulle definizioni degli stessi, sul potere di definizione e sulla reazione sociale.

Oggi, esistono diverse correnti della criminologia critica, a seconda delle dinamiche di potere cui danno maggiore importanza[64].

La criminologia critica è peraltro attenta alle pratiche di resistenza rispetto ai meccanismi di controllo, forte della convinzione che, in ogni caso, i processi di costruzione della criminalità siano essi stessi oggetto di conflitto sociale[65]. Spesso la criminologia critica si è nutrita delle lotte cui gli stessi studiosi e le stesse studiose partecipavano[66].

Inoltre, la criminologia critica è volta a ragionare in un orizzonte di giustizia sociale. Infatti,

> critical criminology rejects as solutions to crime short-term measures such as tougher laws, increased incarceration, coercive counseling therapy, and the like. Rather, critical criminologists regard major structural

---

61 F. Quassoli, *Il sapere dei magistrati: un approccio etnografico allo studio delle pratiche giudiziarie*, in A. Dal Lago, R. De Biasi (a cura di), *Un certo sguardo. Introduzione all'etnografia sociale*, Roma-Bari, Laterza, 2002, pp. 196-217.

62 F. Quassoli, M. Chiodi, *Rappresentazioni sociali e pratiche organizzative di polizia e magistratura*, in *Quaderno n. 21 di Città Sicure*, Regione Emilia-Romagna, 2000, pp. 117-293; G. Fabini, *Polizia e migranti in città: negoziare il confine nei contesti locali*, Roma, Carocci, 2022; F. Quassoli, *"Clandestino": Institutional discourses and practices for the control and exclusion of migrants in contemporary Italy*, in *Journal of Language and Politics*, 2013, 12(2), pp. 203-225; G. Fabini, E. Gargiulo, S. Tuzza, *Polizia: un vocabolario dell'ordine*, Milano, Mondadori Università, 2023.

63 È di questo periodo l'emergere del concetto di intersezionalità: K. Crenshaw, *Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color*, in *Stanford Law Review*, 1991, 43(6), pp. 1241-1299.

64 Per una panoramica in lingua italiana sui differenti filoni di ricerca della criminologia critica si veda C. Rinaldi, P. Saitta (a cura di), *Criminologie critiche contemporanee*, cit.

65 A. Sbraccia, *Criminologie post-coloniale*, cit.

66 D. Melossi, *1977, da Bologna a Berkeley*, in *Studi Sulla Questione Criminale*, 2013, 3, pp. 39-44.

> and cultural changes within society as essential steps to reduce criminality and to promote social justice[67].

La ricerca in criminologia critica è tesa a un orizzonte di giustizia sociale e quindi rifiuta di ricercare la soluzione al problema della criminalità in pene più severe, o in più carcere e più polizia. Al contrario, sono un'organizzazione sociale più giusta e rapporti di potere più equi le chiavi per una diminuzione della criminalità.

La criminologia critica, nelle sue elaborazioni più attuali, ha anche iniziato a prediligere il concetto di danno a quello di crimine[68]. Il ragionamento della zemiologia – il nome che prende la disciplina che studia il danno sociale – è che certi comportamenti, seppur non definiti come criminali, sono in grado di provocare un danno anche più grave di quello provocato da gran parte dei reati e devono essere oggetto di indagine.

Al danno possono essere soggetti non solo individui, ma anche comunità e intere società. A provocarlo possono essere le attività non solo di individui, ma anche di stati nazione, compagnie e imprese locali e statali, regimi politici e ideologie, istituzioni sociali (come ad esempio anche lo stesso sistema della giustizia penale). In questo senso, si rivela come la criminalità non sia in effetti uno dei problemi più stringenti delle nostre società contemporanee. La criminologia critica parte dall'assunto che gli strumenti repressivi quali incarcerazione, controllo di polizia, espulsioni, trattenimento e le pratiche di controllo in senso ampio non solo non siano una soluzione al problema della criminalità, ma anzi provochino essi stessi un danno sociale, che è più utile indagare in questi termini.

Abbiamo quindi visto che la criminologia critica analizza il crimine come risultato di definizioni legali e pratiche di controllo selettivo, interpretando entrambi come espressioni delle strutture di potere diseguali che attraversano la società. Si potrebbe affermare che essa non studia il controllo istituzionale come reazione al crimine, bensì il crimine come effetto del controllo istituzionale in una società intrinsecamente conflittuale e modellata da relazioni di potere. In questo senso, lo studio del crimine – e in particolare delle reazioni sociali al crimine (cioè il sistema penale) – diventa studio delle strutture di potere che governano l'organizzazione sociale.

Questo vale anche nella società digitale, caratterizzata dall'uso pervasivo di big data e sistemi cyber-fisici. Adottando una prospettiva socio-giuridica e cri-

---

[67] W. S. DeKeseredy, B. Perry (a cura di), *Advancing Critical Criminology: Theory and Application*, Lanham (MD), Lexington Books, 2006, pp. 1-2.

[68] P. Hillyard, C. Pantazis, S. Tombs, D. Gordon (a cura di), *Beyond Criminology: Taking Harm Seriously*, London, Pluto Press, 2004.

minologica, è possibile analizzare le complesse interazioni tra tecnologia, diritto e strutture sociali anche nel campo della penalità.

Come abbiamo visto nel paragrafo di apertura, un processo di digitalizzazione pervade la società contemporanee. I dati diventano il nuovo linguaggio del potere, e gli algoritmi si affiancano a (o addirittura sostituiscono) l'agire umano. In questo quadro, la criminologia critica ha il compito urgente di interrogarsi sulla natura delle tecnologie digitali come attori sociali che partecipano attivamente alla costruzione della criminalità e del controllo. La sorveglianza, il riconoscimento facciale, i big data usati per prevenire o reprimere reati non sono solo strumenti: sono pratiche che modificano la stessa definizione di criminalità, agendo a monte della devianza, orientando la percezione collettiva del rischio e innovando le tecniche e le teorie del controllo.

2.5 Criminologia critica digitale

Qui si darà risalto a quelle proposte che recuperano le idee e le posture tipiche della criminologia critica per applicarle allo studio della criminalità e del controllo nella società digitale. Per fare questo, si darà risalto in particolare a tre proposte teoriche, presentate in altrettanti volumi: *Digital criminology. Crime and justice in digital society* di Anastasia Powel, Gregory Stratton e Robin Cameron; *Crime and Punishment in the Future Internet: Digital Frontier Technologies and Criminology in the Twenty-First Century* di Sanja Milivojevic e il *De Gruyter Handbook of Digital Criminology* di Mareile Kaufmann e Heidi Mork Lomell.

Prima di scendere nello specifico di ognuna di queste proposte, conviene soffermarsi sulle loro radici teoriche comuni, che hanno origine in altre discipline e hanno influito sullo sviluppo della criminologia digitale.

L'influenza più profonda arriva forse dagli *Science and Technology Studies* (STS). Gli STS rappresentano un campo interdisciplinare che ha posto al centro della riflessione il rapporto reciproco tra scienza, tecnologia e società. Gli STS criticano l'idea che la tecnologia sia neutrale o autonoma, sottolineando invece il contesto storico, culturale e politico in cui essa si sviluppa e opera. Le tecnologie, in questa prospettiva, non sono solo strumenti ma attori (o meglio, forse, *attanti,* secondo la terminologia di Latour che vedremo a breve) che partecipano attivamente alla trasformazione delle pratiche sociali, dei sistemi normativi e delle istituzioni. L'approccio STS è particolarmente utile per cogliere le conseguenze, le ambiguità e le problematiche etiche generate dall'integrazione delle tecnologie digitali nei processi di controllo.

Un'importante radice teorica della criminologia digitale, nonché del concetto stesso di società digitale, va rintracciata nell'*Actor-Network Theory* (ANT), o *teoria dell'attore-rete*[69]. L'ANT si fonda sull'idea che l'azione sociale non sia prodotta esclusivamente dagli esseri umani, ma da attori eterogenei, umani e non umani, che interagiscono all'interno di reti socio-tecniche. Per questo motivo, Latour preferisce parlare di *attanti* piuttosto che di attori, per sottolineare come qualsiasi elemento – una persona, un oggetto, un algoritmo, un'infrastruttura – possa avere agency. In questa prospettiva, il sociale non è una sfera separata e omogenea, ma un assemblaggio di elementi eterogenei, costantemente riconfigurato da connessioni instabili tra soggetti e oggetti. Il potere, il sapere e l'azione sono quindi performati da configurazioni socio-materiali che includono, necessariamente, le tecnologie come co-produttrici degli esiti sociali. Un esempio di ibrido uomo-macchina con agency propria, riproposto anche da Milivojecvic, è quello dell'uomo con la pistola: né l'uomo da solo, né la pistola da sola sono in grado di produrre un'azione letale, ma *l'ibrido uomo-pistola uccide le persone.* In questo senso, l'ibrido uomo-pistola diventa attante, cioè agente di un'azione specifica. Uno degli insegnamenti fondamentali dell'ANT è che non è possibile determinare a priori quali elementi della rete saranno effettivamente agentivi: l'agency emerge dal contesto specifico della relazione.

Latour[70] ha anche dato un contributo fondamentale alla diffusione del concetto di *black box* nelle scienze sociali, particolarmente utile per pensare la tecnologia nell'era digitale. Con questo termine si riferisce al fatto che le procedure che trasformano gli input in output funzionano come scatole nere, ovvero sono opache, non trasparenti: vediamo solo gli input e gli output, ma non ci interroghiamo su cosa accade nel mezzo. In un contesto altamente digitalizzato, questo effetto di opacità – o "impercepibilità" – diventa sempre più pervasivo: le tecnologie operano costantemente in background, modellano l'azione sociale, ma raramente diventano oggetto di analisi critica.

Esiste un *technological unconscious*[71] che accompagna l'impatto della tecnologia nella vita sociale: la tecnologia c'è e produce degli effetti, ma ce ne dimentichiamo, non ne siamo consapevoli, non sappiamo come funziona e quindi non la consideriamo come determinante degli effetti che essa può avere anche su di noi e sul nostro agire. Ci dimentichiamo della sua esistenza, la naturalizziamo. Proprio contro questa tendenza si collocano le riflessioni più recenti della crimi-

---

69 B. Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*, Oxford, Oxford University Press, 2005.

70 B. Latour, *Science in Action: How to Follow Scientists and Engineers Through Society*, Cambridge (MA), Harvard University Press, 1987.

71 S. Milivojevic, *Crime and Punishment in the Future Internet*, cit.

nologia digitale, che cercano di riportare al centro dell'analisi i processi sociotecnici che co-producono criminalità, controllo e giustizia, superando tanto le visioni umanocentriche quanto quelle deterministe.

Un altro concetto chiave che aiuta a comprendere le trasformazioni contemporanee del controllo sociale, ripreso criticamente sia da Milivojevic che da Powell, Stratton e Cameron, è quello di *ubiquitous surveillance*, ossia sorveglianza ubiqua. Questo concetto, elaborato inizialmente da David Lyon[72] e successivamente approfondito da Mark Andrejevic[73], rappresenta un'evoluzione dei paradigmi precedenti della sorveglianza: dal modello panottico[74], alla sorveglianza post-panottica[75], fino a una nuova forma di sorveglianza diffusa, pervasiva e continua. In questo quadro, la sorveglianza non è più esercitata solo da istituzioni verticali e visibili, ma è automatizzata, decentralizzata, volontaria e integrata nelle pratiche quotidiane della vita digitale. La sorveglianza diventa "ubiqua" perché è ovunque e sempre attiva, resa possibile da ciò che Haggerty ed Ericson[76] definiscono *surveillance assemblage*: un insieme dinamico e interconnesso di tecnologie, attori e dispositivi che aggregano dati sugli individui da fonti diverse (telefoni, carte di credito, videocamere, social media, dispositivi smart). In molti casi, i dati vengono raccolti senza piena consapevolezza, ma spesso anche con il consenso attivo degli utenti, che forniscono informazioni in cambio di servizi digitali, comodità o accesso a piattaforme. Milivojevic sottolinea come questa forma di sorveglianza sia resa ancora più problematica dalla sua opacità: i processi con cui i dati vengono raccolti, elaborati e utilizzati sono in gran parte invisibili, nascosti dentro infrastrutture tecnologiche complesse. Inoltre, come notano Powell, Stratton e Cameron[77], la sorveglianza ubiqua è oggi fortemente intrecciata con processi di privatizzazione e monetizzazione: i dati non sono solo strumenti di controllo, ma risorse economiche, vendute, scambiate e sfruttate da aziende private per profitto, con profonde implicazioni in termini di potere, disuguaglianza e giustizia sociale. In questo contesto, la sorveglianza non è più solo un meccanismo repressivo ma una dimensione strutturale della vita nella società digitale, che pone interrogativi urgenti su *agency*, autonomia, *privacy* e governance algoritmica. La criminologia digitale, in quanto campo cri-

---

72 D. Lyon, *Surveillance studies: An overview, Cambridge*, Polity Press, 2007.

73 M. Andrejevic, *Ubiquitous surveillance*, in K. Ball, K. Haggerty, D. Lyon (a cura di), *The Routledge Handbook of Surveillance Studies*, Abingdon-Oxon, Routledge, 2012, pp. 91-98.

74 M. Foucault, *Sorvegliare e punire. Nascita della prigione*, Torino, Einaudi, 1976.

75 Z. Bauman, *Liquid Modernity*, Cambridge, Polity, 2000.

76 K. Haggerty, R. Ericson, *The surveillant assemblage*, in *British Journal of Sociology*, 2000, 4, pp. 605-622.

77 G. Stratton, A. Powell, R. Cameron, *Crime and justice in digital society*, cit.

tico, è chiamata a interrogare questi dispositivi di potere e a comprendere come contribuiscano alla costruzione e alla gestione della devianza nel presente iperconnesso.

Andiamo adesso nel dettaglio dei tre volumi che abbiamo messo al centro di questo paragrafo.

A livello internazionale, una delle proposte più organiche per la costituzione della criminologia digitale come campo autonomo di ricerca è stata formulata da Greg Stratton, Anastasia Powell e Robin Cameron in un articolo pubblicato nel 2017 sull'*International Journal for Crime and Justice*, intitolato *Crime and Justice in Digital Society: Towards a Digital Criminology*. L'intervento anticipa e sviluppa alcuni temi successivamente approfonditi nel volume collettivo *Digital Criminology* del 2018, firmato dagli stessi autori.

Secondo gli autori e l'autrice, lo sviluppo della ricerca sul cybercrime ha seguito da vicino l'evoluzione delle tecnologie digitali: nella cosiddetta *pre-web era* (anni Ottanta e primi anni Novanta), l'attenzione era rivolta a reati come l'*hacking*, il furto di dati e l'accesso non autorizzato ai sistemi informatici. Con l'avvento della *global web era* (anni Novanta e primi Duemila), l'interesse si è spostato su reati agevolati dall'uso di internet, come le frodi online e la cyberviolenza. Infine, con la diffusione dei social media e delle tecnologie mobili, nella *social web era* (dalla metà degli anni Duemila in poi), la ricerca ha iniziato a esplorare fenomeni come il cyberbullismo, il *dark web*, la sorveglianza digitale e l'uso dei *big data* nelle pratiche di controllo. Tuttavia, sottolineano Stratton, Powell e Cameron, buona parte della letteratura sul cybercrime ha mantenuto un approccio compartimentato, trattando i crimini digitali come semplici estensioni dei reati offline. Questa visione binaria – online versus offline – non coglie la natura profondamente integrata della tecnologia nella vita sociale e nelle pratiche quotidiane. Gli autori e l'autrice propongono quindi di superare questa dicotomia, adottando una prospettiva che consideri l'ambiente digitale non come una dimensione separata, ma come parte costitutiva della realtà sociale. Il loro obiettivo è fondare una criminologia digitale capace di analizzare il crimine, la giustizia e il controllo come fenomeni co-costruiti da relazioni tra soggetti umani, tecnologie e infrastrutture digitali.

Nel delineare i fondamenti teorici di questa proposta, Stratton *et al.* si richiamano a tre approcci critici: la teoria dell'attore-rete (ANT), il postumanesimo e i femminismi post-strutturalisti. Come abbiamo visto, la ANT rifiuta la distinzione rigida tra umano e non umano, attribuendo *agency* anche agli oggetti tecnici, come algoritmi, dispositivi, piattaforme. Nel contesto criminologico, questo significa riconoscere che le tecnologie non sono meri strumenti passivi, ma partecipano attivamente alla produzione del crimine e alle forme di control-

lo. In linea con questa visione, il postumanesimo mette in discussione il primato dell'essere umano come soggetto autonomo e sovrano, sostenendo invece che ogni soggettività è già sempre mediata da relazioni con elementi non umani. I femminismi post-strutturalisti, infine, interrogano le modalità con cui le tecnologie e i saperi normativi costruiscono identità deviate, criminalizzate o marginalizzate, contribuendo alla riproduzione di disuguaglianze strutturali legate a genere, razza e sessualità.

Questa impostazione porta gli autori a concepire la *digital criminology* non come un semplice aggiornamento della criminologia classica, ma come un campo teorico e metodologico nuovo, capace di interrogare le trasformazioni simboliche, materiali e relazionali che ridefiniscono oggi i confini del crimine e della giustizia. In particolare, essi identificano sei aree chiave di indagine:

- *Digital Spectatorship* – l'emergere di forme di partecipazione pubblica ai discorsi sul crimine attraverso i social media, che possono amplificare sentimenti punitivi e disinformazione;
- *Digital Engagement* – l'uso delle piattaforme digitali da parte di gruppi emarginati per contestare le rappresentazioni dominanti della criminalità e rivendicare giustizia;
- *Digital Investigations* – il crescente impiego di dispositivi mobili, tecnologie indossabili e dati digitali nei processi giudiziari, con implicazioni critiche per la privacy e la sorveglianza;
- *Digital Vigilantism* – le pratiche di giustizia informale online (o "digilantismo") che producono forme di stigmatizzazione e violenza simbolica;
- *Embedded Harms* – i danni strutturali generati da piattaforme digitali, come violenze di genere, razziali e sessuali;
- *Digital Inequalities* – le disuguaglianze nell'accesso e nell'uso delle tecnologie, che influenzano tanto la vittimizzazione quanto le possibilità di resistenza.

Attraverso queste direttrici, la criminologia digitale promossa da Stratton, Powell e Cameron si configura come un progetto interdisciplinare, che dialoga con la sociologia, i *media studies*, la filosofia della tecnologia e i *critical data studies*. È una criminologia che si interroga non solo sul crimine "digitale", ma su come il digitale stia trasformando il crimine, la giustizia e le forme di governance nella società contemporanea. Come ricordano gli autori, ciò significa anche ripensare il ruolo della tecnologia, mettendo in discussione la sua presunta neutralità e interrogando i processi attraverso cui le categorie di crimine e controllo vengono costruite socialmente, culturalmente e politicamente.

Secondo in ordine di tempo, un contributo originale e teoricamente denso alla riflessione sulla criminologia digitale proviene dal lavoro di Sanja Milivojevic, che propone di affrontare l'impatto delle *digital frontier technologies* (DFTs) su criminalità, vittimizzazione e controllo sociale attraverso una prospettiva interdisciplinare, speculativa e critica. Il volume adotta tecniche tipiche del campo dei *foresight studies*, come lo *scanning* e la *scenario writing* trattandole come veri e propri metodi qualitativi per esplorare i futuri possibili. Lo *scanning* si configura come un'osservazione sistematica delle trasformazioni tecnologiche, socio-culturali, economiche e normative, fondata su analisi bibliografiche, fonti politiche e ricerche bibliometriche. La *scenario writing*, invece, consente di costruire narrazioni plausibili su sviluppi futuri a partire dall'analisi del presente, elaborando domande del tipo "cosa accadrebbe se...?". Come chiarisce Milivojevic, «in questo libro adotto uno scenario esplorativo che pone domande del tipo 'e se questo accadesse': osservo gli sviluppi possibili delle DFTs, analizzo e ipotizzo 'storie future' e delineo scenari probabili relativi al crimine, all'offesa e al controllo»[78].

Queste tecniche, che Milivojevic propone di integrare nella ricerca criminologica, derivano in parte dagli *Science and Technology Studies* (STS), sopra citato. Proprio su questo punto si innesta la riflessione di Milivojevic: la criminologia, osserva l'autrice, si è concentrata prevalentemente su fenomeni consolidati come il cybercrime, la sorveglianza o le frodi digitali, trascurando il potenziale trasformativo – e le implicazioni sistemiche – delle DFTs. Raramente ci si è interrogati su quali possano essere gli effetti futuri di temi cruciali come *big data*, *privacy*, sicurezza e sorveglianza. Per affrontare tali sfide, l'autrice propone un'integrazione tra approccio empirico (*scanning*), immaginazione speculativa (scenario writing) e cornici teoriche critiche, come la Actor-Network Theory, appunto, ma anche il concetto di *black box*, quello di *technological unconscious*, l'idea di *ubiquitous surveillance*.

Il cuore dell'argomentazione riguarda però una trasformazione più radicale, che mette in discussione i presupposti stessi della criminologia. L'avanzamento delle DFTs comporta un mutamento delle forme di *agency*:

> per troppo tempo, come ci ricorda Janet Chan (2018), abbiamo trascurato l'importanza delle cose: algoritmi, dispositivi di sicurezza, muri. Ci siamo concentrati sugli esseri umani e sull'impatto che hanno su crimine, vittimizzazione e controllo. Oggi non possiamo più ignorare l'espansione e l'agency delle tecnologie. Dobbiamo ripensare il nostro ruolo nel mon-

[78] S. Milivojevic, *Crime and Punishment in the Future Internet*, cit., p. 8.

> do tecno-sociale del crimine e della vittimizzazione, e considerare perché è essenziale ritrovare il nostro posto nell'equazione[79].

In questa prospettiva, la tecnologia non è più un semplice ausilio o un ambiente: diventa co-costitutiva dei fenomeni criminali e dei dispositivi di controllo. L'alleanza umano-tecnologica che ha definito la modernità rischia di essere sostituita da una crescente alleanza tra tecnologie, in cui gli umani assumono un ruolo marginale nella produzione e gestione del rischio. La criminologia critica è dunque chiamata a riformulare le proprie categorie analitiche, interrogando chi – o cosa – agisce, decide, punisce e protegge in un mondo iperconnesso e automatizzato.

L'autrice sottolinea come la criminologia tradizionale si sia limitata a tematizzare fenomeni ormai consolidati – come il cybercrime, la sorveglianza o le frodi digitali – trascurando però le implicazioni più profonde delle DFTs sul lungo periodo. Per colmare questa lacuna, Milivojevic propone un cambio di prospettiva: ripensare il ruolo della criminologia all'interno del mondo tecnosociale, abbandonando la centralità esclusiva dell'agire umano e aprendosi a una considerazione più ampia dell'agency tecnologica. In questa cornice, l'autrice riprende la lezione di Latour e della Actor-Network Theory, così come di altri approcci affini, per interrogarsi su un mondo in cui le decisioni saranno sempre più mediate da algoritmi, automatismi e dispositivi connessi, e in cui l'umano potrebbe essere progressivamente escluso dalla scena decisionale. Milivojevic insiste tuttavia su un punto fondamentale: l'agency non coincide con l'intenzione. Le tecnologie hanno effetti, ma non interessi propri – almeno non ancora. Tuttavia, l'erosione dell'alleanza tra umano e "cosa" rischia di lasciare spazio a un nuovo equilibrio, in cui l'alleanza tra tecnologie potrebbe diventare dominante, con conseguenze radicali per il crimine e il suo governo.

In definitiva, questo libro non offre risposte definitive, ma piuttosto apre una nuova prospettiva critica sulla criminologia del futuro, invitando a reinserire l'umano nell'equazione e a sviluppare un pensiero più ampio e teoricamente informato sulle intersezioni tra giustizia penale, tecnologia e società.

Nel contesto delle trasformazioni indotte dalle tecnologie digitali, Sanja Milivojevic propone un posizionamento teorico che si colloca all'interno del dibattito sul rapporto tra tecnologia e società, richiamando una tipologia a tre approcci elaborata da Matthewman[80]. Il primo è il determinismo tecnologico, secondo cui la tecnologia sarebbe una forza autonoma, neutra e razionale, ca-

---

79 Ivi, pp. 11-12.

80 S. Matthewman, *Technology and Social Theory*, Basingstoke, Palgrave Macmillan, 2011.

pace di guidare da sola il progresso umano lungo una traiettoria inevitabile. Il secondo è l'approccio umanista, che invece pone al centro l'essere umano come soggetto agente e responsabile: le tecnologie non si sviluppano da sole, ma in risposta a esigenze sociali, culturali o pratiche. Un esempio spesso citato a sostegno di questa posizione è lo sviluppo della bicicletta moderna, che ha preso forma per soddisfare una domanda di maggiore sicurezza, sostituendo i modelli precedenti con grandi ruote frontali. Infine, il terzo approccio – quello che Milivojevic abbraccia – è il postumanesimo, secondo cui l'agency non è esclusiva né dell'umano né della tecnologia, ma è distribuita all'interno di assemblaggi tecno-sociali. In questa prospettiva, le tecnologie non sono strumenti passivi, ma veri e propri *attanti*, capaci di influenzare, condizionare e co-costruire la realtà sociale insieme agli esseri umani. Ciò implica un ripensamento radicale del rapporto tra soggetto, oggetto e contesto: umani e non umani sono co-agenti nei processi di trasformazione sociale.

Milivojevic applica questo quadro al tema delle Digital Frontier Technologies (DFTs) e del futuro della società digitale. Sottolinea come l'equilibrio tra umano e macchina, finora simmetrico, sia potenzialmente messo a rischio dallo sviluppo accelerato delle tecnologie all'interno di un *milieu* dominato dai big data e dalla sorveglianza. La domanda che solleva è cruciale: «lo sviluppo delle DFTs, nel contesto più ampio dei big data e della sorveglianza, minaccerà l'equilibrio tra esseri umani e tecnologia al punto da ridurre l'agency umana, mentre l'impatto della tecnologia su vita, salute, criminalità, vittimizzazione e penalità continuerà a crescere?»[81].

In questa visione, strumenti come gli smartphone non sono solo oggetti di uso quotidiano, ma dispositivi che modellano le abitudini, i comportamenti e persino l'identità umana, così come, viceversa, sono essi stessi modellati dalle esigenze, dai desideri e dalle pratiche sociali. Il postumanesimo, dunque, offre una lente potente per analizzare come la criminalità e il controllo si riformulano all'interno di questa relazione dinamica e reciproca tra umano e tecnologia, che non può più essere pensata in termini di causalità lineare o di semplice strumentalità.

Da ultimo, recentissimo, è il lavoro di sistematizzazione del lavoro empirico e teorico condotto in questo campo emergente di studi, la criminologia digitale, curato da Kaufmann e Lomell. Il *De Gruyter Handbook of Digital Criminology* rappresenta il primo manuale di criminologia digitale mai pubblicato: un lavoro mastodontico, in open access, di più di 500 pagine e con più di 50 contributi sui più svariati temi, sia teorici che empirici. Il collettaneo si distingue per il modo

[81] S. Milivojevic, *Crime and Punishment in the Future Internet*, cit., p. 12.

in cui propone di ripensare radicalmente le basi epistemologiche e ontologiche della criminologia stessa, alla luce della trasformazione digitale della società. Secondo le curatrici, il digitale non rappresenta più un oggetto di studio esterno o una "nuova frontiera" per le teorie già esistenti, ma costituisce un elemento strutturale della realtà sociale contemporanea, che trasforma in profondità cosa intendiamo per crimine, chi è coinvolto nei processi di controllo e in che modo la giustizia viene esercitata. La *digital criminology* viene quindi concepita non come sottodisciplina tematica (limitata, per esempio, allo studio del cybercrime), ma come una prospettiva teorica che obbliga la criminologia a rivedere le proprie categorie fondative. Innanzitutto, proprio come negli altri lavori che abbiamo presentato in questo paragrafo, viene criticata la distinzione netta tra online e offline, una dicotomia che non regge più alla prova delle pratiche sociali e tecnologiche integrate. La società contemporanea è immersa in un ambiente iperconnesso, dove il digitale non è un "altrove", ma si intreccia in modo costitutivo con le vite materiali, affettive, economiche e politiche delle persone. In questo contesto, le tecnologie non possono più essere considerate strumenti neutri, ma vanno intese come agenti attivi, capaci di modellare il comportamento, la percezione del rischio, le relazioni di potere e le stesse definizioni di devianza.

Un punto particolarmente rilevante dell'approccio proposto da Kaufmann e Lomell riguarda il carattere situato e non neutrale del sapere criminologico. Le autrici insistono sulla necessità di riconoscere che ogni produzione di conoscenza – inclusa quella scientifica – parte da una posizione e che il sapere criminologico partecipa, in molti casi, alla costruzione di classificazioni, narrazioni e pratiche di controllo che non sono affatto innocenti. In questo senso, la *digital criminology* si configura come una criminologia critica, riflessiva, consapevole del proprio ruolo nei processi di governance digitale.

La posta in gioco, in questo cambio di paradigma, è tanto teorica quanto politica: non si tratta solo di comprendere come cambia il crimine con il digitale, ma di interrogarsi su chi viene reso visibile o invisibile, su quali soggettività vengono profilate, criminalizzate, neutralizzate o escluse, e su quali forme di giustizia siano ancora possibili in un mondo governato da algoritmi, piattaforme e infrastrutture opache. L'approccio proposto nel manuale invita a pensare la criminologia non solo "nel digitale", ma attraverso il digitale, mettendo al centro l'intreccio tra potere, sapere e tecnologia che caratterizza la società contemporanea.

3. *Datification* tra produzione e controllo della criminalità

3.1 Cosa sono i big data

Fornire una definizione del concetto di big data è molto più complesso di quanto non sembri in apparenza. Può voler dire riferirsi ai dataset, agli algoritmi che lo regolano, alla realtà tecnica o anche al portato culturale. Come scrivono Chan e Bennet Moses,

> È possibile definire i *Big Data* facendo riferimento alla dimensione e al tipo di dataset utilizzati, alle capacità dei sistemi di archiviazione, elaborazione e/o analisi dei dati, come un insieme di promesse di marketing su ciò che determinate tecnologie dichiarano di consentire,[1] oppure come un fenomeno sociale e culturale. La ragione della molteplicità di definizioni sta nella varietà delle tecnologie impiegate, delle piattaforme e dei sistemi potenzialmente coinvolti, così come negli obiettivi che si intendono raggiungere. L'etichetta "Big Data" cattura dunque una tendenza generale nel modo in cui i dati vengono raccolti, archiviati e utilizzati, piuttosto che identificare un prodotto o un processo specifico[2].

---

[1] Nella versione originale di questa citazione si parla di «as a set of marketing claims about what is enabled by particular technologies», probabilmente con riferimento al fatto che il termine *Big Data* viene usato anche come slogan promozionale, cioè come termine-ombrello che raccoglie affermazioni esagerate o persuasive su ciò che certe tecnologie permettono di fare, indipendentemente dalla realtà tecnica. In questo senso, "Big Data" può indicare anche un insieme di promesse commerciali formulate dalle aziende tecnologiche per vendere software e servizi legati all'analisi dei dati.

[2] J. Chan, L. Bennett Moses, *Is Big Data challenging criminology?*, in *Theoretical Criminology*, 2016, 20(1), p. 24.

Con big data, si fa riferimento, quindi, più in generale a un processo di *datificazione*[3] tipico dell'era digitale attuale. Un processo che coinvolge tutte le interazioni sociali e tramite il quale le interazioni vengono trasformate in numeri[4].

Volendo però provare in ogni caso a fornire una definizione del concetto di big data, solitamente chi si occupa di questo tema prova innanzi tutto a darne una tecnica.

Tecnicamente, una maniera popolare di definire i big data ricorre alle tre V: Volume, Velocità, Varietà[5]. La prima dimensione, il Volume, fa riferimento alla possibilità di raccogliere, archiviare e processare una quantità enorme di dati, prima inimmaginabili, ben oltre le capacità tradizionali. La seconda dimensione, la Velocità, fa riferimento al fatto che questa gran mole di dati può essere analizzata e processata in tempo (quasi) reale. La terza dimensione, la Varietà, fa invece riferimento a che tipo di dati sono contenuti in questi *dataset*: sono dati sempre più vari, provenienti da fonti sempre più diversificate, che usano format diversi e hanno strutture dissimili. I dati non provengono solo da registri ufficiali, ma da fonti eterogenee come social media, dispositivi cyberfisici di vario tipo, videocamere a circuito chiuso, smart phone, dispositivi di tracciamento GPS, acquisti online, le tessere di fedeltà che continuiamo a sottoscrivere, le nostre ricerche sul web, ecc.[6]. Quasi ogni cosa che facciamo lascia tracce elettroniche. Come scrive Milivoijevic,

> nel nostro micro-universo produciamo un'enorme quantità di dati ogni singolo giorno. Da quando ci svegliamo a quando andiamo a dormire, una serie di artefatti ci osserva, archivia, scambia e analizza costantemente dati su di noi e sulle nostre attività. I dati sono un backlog, un racconto della nostra esistenza – quello che, a volte, non possiamo cancellare[7].

Però qui si nasconde un'insidia: nei big data si accostano dati molto diversi tra loro, che non sono stati né raccolti né codificati nello stesso modo e, dunque, non risultano subito leggibili nel loro insieme. Non sono subito accostabili. Inoltre, sono dati "sporchi", che devono essere quindi puliti, classificati e riordi-

---

3 J. Van Dijck, *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, in *Surveillance and Society*, 2014, (12), pp. 197-208.

4 B. Aragona, S. Stefanizzi, *Società digitale: interrogativi, aree di ricerca e ruolo della sociologia*, cit.

5 L. Bennett Moses, J. Chan, *Using Big Data for legal and law enforcement decisions: testing the new tools*, in *UNSW Law Journal*, 2014, 37(2), pp. 643-678; J. Chan, L. Bennett Moses, *Is Big Data challenging criminology?*, cit.

6 D. Lupton, *Digital Sociology*, London, Routledge, 2015; G J.D. Smith, P. O'Malley, *Driving politics: Data-driven governance and resistance*, in *British Journal of Criminology*, 2017, 57(2), pp. 275-298.

7 S. Milivojevic, *Crime and Punishment in the Future Internet*, cit., p. 17.

nati per poter essere utilizzabili. In questo senso, Milivojevic parla dei big data come del nuovo petrolio.

L'accostamento tra big data e petrolio era stato proposto per primo da un matematico inglese, Clive Humby, nel 2006, proprio per il potere che avere accesso e detenere il controllo dei big data produce nella contemporaneità[8]. Milivojievic aggiunge tuttavia altri elementi a questa metafora: proprio come il petrolio, anche i big data devono essere ripuliti, riorganizzati, riordinati per fare in modo che abbiano valore. Cioè, «i big data, come il petrolio, non possono essere utilizzati fino a che non vengono raffinati»[9].

Anche sul volume e sulla velocità che caratterizzano la definizione tecnica di big data si possono avanzare delle riflessioni. La definizione di *big data* è relativa e dinamica[10], ovvero ciò che conta come estremamente grande, efficiente, flessibile, vario e mobile, è un target variabile: ciò che in passato veniva percepito come un dataset enorme, oggi può apparire modesto rispetto alle capacità tecnologiche attuali[11]. Dunque, il volume che caratterizza i big data non è mai una misura fissa, ma cambia insieme allo sviluppo delle tecnologie di raccolta e di archiviazione. Ovvero, con l'avanzare della capacità di calcolo e della memoria digitale, la soglia di ciò che viene considerato "big" si sposta sempre più in alto.

Il concetto stesso di "big" è legato non solo al volume in senso quantitativo, ma alla possibilità di processare in tempo reale dati provenienti da fonti eterogenee: ciò che segna la differenza non è un numero assoluto di informazioni, ma la capacità tecnologica di tracciarle, archiviarle e soprattutto analizzarle. Gran parte della tecnologia è volta a velocizzare i tempi del *data-process,* a ridurre il tempo necessario affinché questi dati possano essere letti e, dunque, diventare intellegibili. In passato, dataset che oggi considereremmo piccoli venivano percepiti come enormi rispetto alle capacità di analisi disponibili allora. Tuttavia, con la potenza di calcolo e gli spazi di archiviazione disponibili oggi, tali dataset non sono più considerati "big", mentre lo diventano quelli che raccolgono miliardi di dati provenienti da telefoni cellulari, social media, telecamere di sorveglianza o sensori urbani. I big data sono un concetto relativo e tecnologicamente situato: ciò che è big oggi potrebbe essere "ordinario" domani[12].

---

8 Citato in D. Wall, *How big data feeds big crime*, in *Global His. J. Contemp. World Aff.*, January 2018, pp. 29-34, p 29.

9 S. Milivojevic, *Crime and Punishment in the Future Internet*, cit., p. 18.

10 G. Ferguson, *The Rise of Big Data Policing. Surveillance, race and the future of law enforcement*, New York, New York University Press, 2017.

11 J. Chan, L. Bennett Moses, *Is Big Data challenging criminology?*, cit.

12 G. Ferguson, *The Rise of Big Data Policing*, cit.

Risulta possibile quindi affermare che per essere definito big data, un dataset deve avere una dimensione che rende impossibile ai software classici archiviarlo, gestirlo, analizzarlo[13]. In questo senso, big data è una definizione sempre al limite delle frontiere digitali, nel senso che è big data fintanto che la tecnologia tramite cui i dataset vengono processati non avanza così tanto da rendere i software niente più che strumenti comuni, tipici. Proprio per questo, perché gli strumenti tecnologici sono per loro natura mutevoli e cambiano ad una velocità incrementale, nel suo lavoro Milivoijevic preferisce parlare di *Digital Frontiers Technologies* (DFTs).

Fino ad ora ci siamo soffermati sulla definizione tecnica dei big data, che pone al centro dell'analisi questioni, come la sicurezza dei dati, il costo del processare i dati, l'efficienza dei processi di analisi, la maniera in cui diversi dataset con differenti strutture e diversi formati possono essere combinati, o anche resi interoperabili.

Le definizioni tecniche hanno talvolta fatto riferimento a ulteriori dettagli. Ad esempio, Zavrsnik ha aggiunto altre V alle 3 classiche che abbiamo già visto (Volume, Velocità, Varietà). Nello specifico: *Veracity*, Valore e Vulnerabilità[14]. Kitchin si concentra invece su altre caratteristiche. Egli ritiene che per essere considerati big data, i dataset dovrebbero essere esaustivi nel loro ambito di riferimento, ovvero dovrebbero essere in grado di catturare i dati riguardanti un intero territorio o un'intera popolazione, non solo un campione di quel territorio o di quella popolazione. Oltre ad essere esaustivi, i big data dovrebbero essere ad alta risoluzione, cioè capaci di fornire informazioni molto dettagliate. Dovrebbero avere poi una natura individualizzante, perché possono essere collegati a persone o oggetti specifici, e non solo a categorie generiche. Sono anche relazionali, nel senso che possono essere incrociati e messi in relazione con altri dataset, permettendo nuove forme di analisi. Infine, sono flessibili, cioè strutturati in modo da poter essere continuamente ampliati, sia aggiungendo nuove variabili sia aumentando la loro dimensione complessiva[15].

Secondo Sarah Bryne, una sociologa statunitense che ha studiato l'utilizzo dei big data da parte della polizia di Los Angeles, il concetto di big data ha una definizione più tecnica (quella delle tre V) e una colloquiale. In termini colloquiali, "big data" coincide grossomodo con grandi quantità di dati macinate da

---

[13] J. Manyika *et al.*, *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, McKinsey Global Institute, giugno 2011.

[14] d. boyd, K. Crawford, *Critical questions for Big Data*, in *Inf. Commun. Soc.*, 2012, 15(5), pp. 662-679; A. Završnik (a cura di), *Big Data, Crime and Social Control*, London-New York, Routledge, 2018.

[15] R. Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*, Los Angeles-London-New Delhi-Singapore-Washington D.C., SAGE Publications, 2014.

computer potenti per scovare associazioni che altrimenti non vedremmo. Brayne adotta una definizione che combina l'aspetto tecnico e quello comune: al cuore, secondo la studiosa, i big data sono un ambiente informativo reso possibile dalla digitalizzazione di massa e associato all'uso di analitiche avanzate (come l'analisi di rete e il *machine learning*). In parallelo, anche "algoritmo" ha un doppio registro: tecnicamente è un insieme formale di istruzioni usate per analizzare dati e automatizzare decisioni (spesso paragonato a una "ricetta"); nell'uso corrente indica più in generale il processo attraverso cui i computer prendono decisioni automatiche e predittive su un dataset[16].

Ancora più interessante risulta essere la definizione epistemologica e culturale di big data elaborata da boyd e Crawford, ripresa da vari autori e autrici. Secondo tale definizione, i big data sarebbero anche un fenomeno culturale, tecnologico e mitologico, ovvero offrirebbero la convinzione che i big data siano in grado di fornire verità oggettive e infallibili[17]. Secondo le parole delle due autrici, la mitologia riguarda «la credenza diffusa che i grandi dataset offrano una più alta forma di intelligenza e sapere che può generare conoscenze precedentemente impossibili, con una aurea di verità, oggettività e accuratezza»[18]. Questa mitologia si basa sull'idea che l'analisi di grandi quantità di dati possa produrre una conoscenza "superiore", apparentemente oggettiva e neutrale, capace di sostituire la teoria. Ma, per l'appunto, questa è una mitologia, una credenza diffusa che dimentica il fatto che esistono dei processi di costruzione dei dati e degli algoritmi che non possono essere neutri.

Chan e Bennet Moses spiegano bene questa criticità. Riprendendo per l'appunto questa idea di boyd e Crawford, Chan e Bennett Moses mettono in discussione la mitologia della neutralità dei big data, sottolineando che ogni fase del trattamento dei dati (raccolta, classificazione, analisi), anche quando si presenta come puramente tecnica o "neutra", incorpora presupposti teorici impliciti in ogni fase del processo[19]. Questo vale per la raccolta dei dati, poiché decidere *quali* dati raccogliere implica una scelta basata su ciò che si considera rilevante o utile. Ad esempio, raccogliere dati sui luoghi di reato, ma non su fattori socioeconomici, presuppone una certa visione di cosa sia importante per comprendere il crimine. Questo vale anche per la struttura e il formato dei dati, poiché la necessaria opera di organizzazione e classificazione dei dati non è mai neutra. Le autrici fanno notare che le modalità con cui i dati sono definiti, categorizzati

16 S. Brayne, *Predict and Surveil. Data, discretion and the future of policing*, New York, New York University Press, 2021.

17 d. boyd, K. Crawford, *Critical questions for Big Data*, cit.

18 Ivi, pp. 662-663.

19 J. Chan, L. Bennett Moses, *Is Big Data challenging criminology?*, cit.

e salvati riflettono una certa ontologia—cioè un modello implicito su come il mondo è strutturato. Questo vale anche per la scelta degli strumenti analitici: gli algoritmi usati (come le *random forests* nel *machine learning*) sono costruiti su teorie statistiche e modelli di apprendimento che, sebbene spesso trattati come meri strumenti, incorporano visioni specifiche su come interpretare i dati. Anche la selezione delle variabili da includere nei modelli è guidata da ipotesi – esplicite o tacite – su cosa possa influire sul fenomeno osservato. E, infine, questo vale anche per l'interpretazione dei risultati. Infatti, anche quando l'obiettivo è solo la previsione (e non la spiegazione causale), i pattern individuati vengono inevitabilmente messi in relazione con teorie, anche se in modo implicito. Le autrici osservano che i risultati "parlano" solo se l'analista ha un quadro teorico entro cui collocarli. Su questo torneremo più in dettagli nel paragrafo 3.5. Per ora, basti osservare che ogni fase è carica di scelte interpretative che richiedono riflessione teorica, anche quando questa non è esplicitamente dichiarata.

3.2 Come vengono costruiti i big data

Una volta stabilito cosa siano i big data, proviamo a vedere come questi dataset vengono costruiti.

Sono tre principalmente i modi in cui i dati vengono collezionati e immessi in questi immensi archivi digitali[20]. La prima modalità è sostanzialmente automatica, ovvero i dati vengono creati senza che noi ce ne rendiamo conto. Ciò può avvenire attraverso gli smartphone, dato che ogni volta che usiamo il telefono vengono registrati dati su posizione GPS, app usate, tempi di utilizzo, contatti. Questi dati vengono raccolti automaticamente in background, senza che noi li inseriamo manualmente. Oppure, quando utilizziamo i social media, ogni like, condivisione o commento alimenta dataset giganteschi, che registrano non solo ciò che pubblichiamo, ma anche il tempo trascorso a guardare un contenuto, la velocità con cui scorriamo la pagina, o le interazioni con certi profili. Ogni transazione che effettuiamo con carte di credito o tramite pagamenti digitali viene registrata in automatico, creando database che non solo tengono traccia delle spese, ma le collegano a luoghi, orari e categorie di acquisto. Dispositivi cyberfisici, come termostati intelligenti, smartwatch, braccialetti fitness, aspirapolveri robot e assistenti vocali, collegati a noi ma anche tra loro tramite l'internet delle cose, registrano continuamente dati (temperatura, battito cardiaco, passi, planimetria di casa, comandi vocali). Nell'e-commerce, piattaforme

[20] S. Milivojevic, *Crime and Punishment in the Future Internet*, cit.

commerciali creano dataset dettagliatissimi che collegano ricerche, click, acquisti, tempi di permanenza sulle pagine, recensioni scritte e persino prodotti messi nel carrello e poi abbandonati. In tutti questi casi i dataset non vengono creati da noi in senso attivo, ma vengono generati passivamente da sistemi digitali che registrano ogni interazione e la traducono in dati. Questi sono processi automatici ("automated") di generare big data, processi tramite cui i dati vengono creati autonomamente senza interferenza[21].

Una seconda modalità tramite cui i dati vengono raccolti in questi dataset si deve a una nostra scelta deliberata. Se prima abbiamo visto i dati che cediamo in modo "passivo" (senza rendercene conto), ci sono anche moltissime situazioni in cui li forniamo "volontariamente", spesso in cambio di un servizio, di comodità o di piccoli vantaggi. Nei social network (Facebook, Instagram, TikTok, X), ogni volta che postiamo foto, commenti, preferenze politiche o like, decidiamo attivamente di condividere informazioni che arricchiscono i database delle piattaforme. Utilizzando le tessere di fedeltà (supermercati, farmacie, librerie), accettiamo di lasciare tracce dettagliate dei nostri acquisti in cambio di sconti, punti o promozioni personalizzate. Usufruendo di servizi di streaming (Spotify, Netflix, ecc.), stiamo contribuendo alla costruzione di dataset sui nostri gusti e abitudini culturali nel momento in cui creiamo playlist, diamo valutazioni o scegliamo cosa guardare. Tramite le app di navigazione o fitness (Google Maps, Strava) condividiamo percorsi, tempi di percorrenza, dati sul traffico o sul nostro corpo (battito cardiaco, calorie, sonno) perché l'app ci restituisca un servizio utile. Durante gli acquisti online (Amazon, Zalando, ecc.), oltre a comprare, spesso lasciamo recensioni, preferenze di consegna, liste dei desideri: tutti dati che arricchiscono enormemente i profili personali costruiti dalle piattaforme. Anche partecipando a quiz e giochi online, come test di personalità, giochi su Facebook o sondaggi, spesso consentiamo l'accesso ai nostri profili e alle nostre liste di contatti; così come quando ci iscriviamo a una newsletter o accettiamo condizioni di servizio: nel farlo forniamo volontariamente indirizzi e-mail, numeri di telefono o interessi. In tutti questi casi la cessione è consapevole, "volontaria", anche se raramente ci soffermiamo a riflettere sul fatto che stiamo scambiando dati personali per servizi: convenienza, intrattenimento, sconti, visibilità sociale.

La terza modalità, invece, riguarda i dati che vengono raccolti direttamente dalle forze dell'ordine o da altre istituzioni, senza che siano né generati automaticamente dai dispositivi, né ceduti volontariamente dai cittadini. Per fare alcuni esempi, si tratta dei dati raccolti tramite CCTV e videosorveglianza. Le

[21] R. Kitchin, *The Data Revolution*, cit.

telecamere installate in spazi pubblici o privati registrano immagini che vengono poi archiviate e, in certi casi, analizzate con software di riconoscimento facciale o di tracciamento dei movimenti. Oppure, durante un controllo di polizia in macchina o a piedi, gli e le agenti raccolgono dati diretti come patente, documenti di identità, numero di targa, eventuali dichiarazioni. Anche durante i pattugliamenti, le e gli agenti possono prendere appunti o compilare rapporti su comportamenti osservati in strada (es. "persone sospette in sosta in un'area"), che vanno a popolare database di intelligence. Nei paesi dove sono adottate, le bodycam registrano in diretta l'interazione tra polizia e cittadini, producendo dataset audiovisivi molto dettagliati. Anche autovelox, telecamere per il controllo delle targhe, varchi elettronici per l'accesso alle città generano dati diretti, destinati a essere utilizzati per fini sia amministrativi che di polizia. Anche durante controlli amministrativi, come sopralluoghi di ispettori del lavoro, controlli doganali o ispezioni fiscali, i dati vengono raccolti manualmente e inseriti in database istituzionali. In questo caso, a differenza dei dati "ceduti passivamente" o "ceduti volontariamente", siamo di fronte a una raccolta diretta e intenzionale da parte di autorità o organizzazioni, con finalità di sorveglianza, prevenzione o controllo.

Una volta collezionati, questi dati sono posseduti da vari attori: sviluppatori di software, compagnie private, pubblicitari, banche, polizia, governi e tanti altri. Esiste un vero e proprio mercato dei dati personali, gestito da società private note come *data broker*. Queste imprese raccolgono, acquistano e rivendono informazioni su milioni di persone: i dati possono servire ad aziende commerciali per produrre pubblicità mirata, alle banche per valutare l'affidabilità creditizia o ai datori di lavoro per controllare i candidati. Ma lo stesso flusso informativo può essere venduto anche alle forze dell'ordine, che lo utilizzano a fini di indagine[22]. Il valore dei dati e l'importanza di possederli sono così alti che, per l'appunto, qualcuno come abbiamo già visto parla dei big data come del nuovo petrolio. Qualcun altro invece ha coniato il termine di capitalismo della sorveglianza[23].

Un altro elemento fondamentale da tenere in considerazione quando pensiamo ai processi di costruzione dei big data è che, lungi dall'essere una rappresentazione neutrale della realtà, fondata sulla sua oggettività scientifica, i dati sono socialmente costruiti. Essi, infatti, esistono attraverso l'azione sociale e non prima di essa[24]. Su questo punto insiste molto anche Sarah Brayne[25]. Uno

---

22 G. Ferguson, *The Rise of Big Data Policing*, cit.

23 S. Zuboff, *Big other: Surveillance capitalism and the prospects of an information civilization*, in *Journal of Information Technology*, 15, 3, pp. 75-89.

24 G.C. Bowker, *Data Flakes: An Afterword to "Raw Data" is an Oxymoron*, in L. Gitelman (a cura di), *'Raw Data' Is an Oxymoron*, Cambridge, MA, MIT Press, 2013, pp 167-172.

25 S. Brayne, *Predict and Surveil*, cit.

dei punti di partenza della sua analisi è che, checché ne dica la retorica che parla di neutralità del dato, il dato non è neutro: non è neutra la maniera in cui viene costruito, la maniera in cui viene usato, e non è neutro il sistema sociale entro cui il sistema di rilevamento del dato viene costruito.

Il processo sociale di costruzione del dato è ancora più rilevante nel momento in cui ci rendiamo conto del fatto che i dati una volta prodotti diventano autonomi, non hanno memoria delle proprie origini e sono indipendenti rispetto alle procedure di produzione che li hanno riguardati. Nell'economia dei dati digitali, i dati hanno una vitalità propria[26]. Come sostiene Lupton, hanno una propria vita sociale distinta dagli esseri umani che li hanno generati[27]. Il rischio è quindi che i processi di produzione dei dati rimangano invisibili e che dunque venga invisibilizzata l'asimmetria di potere tramite cui i dati vengono creati mentre rimane visibile solo la conoscenza che da quei dati si può trarre. Una conoscenza presentata come neutrale ma che non lo è davvero, forte dell'oblio del processo di costruzione del dato. Infatti, i dati una volta prodotti circolano, danno la possibilità di produrre diverse forme di conoscenza e possono essere utilizzati e ripresentati in svariati modi tra loro differenti.

Questo vale tanto per i big data quanto per gli algoritmi utilizzati per processarli. Nel dire big data, infatti, inevitabilmente, come abbiamo visto nel paragrafo precedente, facciamo riferimento sia alla massiva archiviazione digitale sia ai software di data mining, ovvero i software utilizzati per estrapolare conoscenza da quei dati (si veda il par. 3.5).

Qui allora ci viene in aiuto Zavrsnik e il suo articolo *Algorithmic justice: Algorithms and big data in criminal justice settings*, dove, tra le molte questioni affrontate, troviamo una discussione critica su come i database e gli algoritmi vengano creati nel contesto della giustizia penale e quali rischi ne derivino[28].

Secondo Završnik, la costruzione di database e algoritmi in ambito penale non è un processo neutrale, ma un'attività profondamente umana e politica: non esistono dati "neutri", ma scelte su cosa raccogliere, come etichettare e come interpretare. Tali scelte riflettono valori e priorità. Završnik riprende, innanzitutto, l'osservazione di Cathy O'Neil la quale, nel noto *Weapons of Math Destruction*, sottolinea come «i modelli siano opinioni incorporate nella matematica»[29]. Questa riflessione evidenzia che i software di analisi non sono

---

[26] B. Aragona, S. Stefanizzi, *Società digitale: interrogativi, aree di ricerca e ruolo della sociologia*, cit.

[27] D. Lupton, *Digital sociology*, cit.

[28] A. Završnik, *Algorithmic justice: Algorithms and big data in criminal justice settings*, in *European Journal of Criminology*, 2019, 18, 5, pp. 632-642.

[29] C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, Crown Random House, 2016.

strumenti imparziali, bensì veicolano le concezioni di chi li ha creati. In secondo luogo, Završnik sottolinea che l'affidabilità dei sistemi predittivi dipende anche dalla qualità dei dati di partenza. Nel settore della giustizia penale, tuttavia, i dati risultano spesso parziali o distorti. Una prima ragione di ciò è il cosiddetto numero oscuro della criminalità.

La criminalità può essere distinta in criminalità registrata (quella denunciata e quindi rilevata dalle statistiche ufficiali) e criminalità nascosta (quella non denunciata, che rimane invisibile ai sistemi istituzionali di rilevazione). La criminalità reale è dunque la somma di entrambe. La percentuale di criminalità nascosta rispetto a quella registrata varia a seconda del reato. Alcuni reati vengono infatti denunciati più spesso, altri più raramente. Le cause sono molte e diverse: non si denuncia per vergogna, come nel caso di alcune violenze sessuali o di truffe; non si denuncia perché non si è consapevoli di essere vittima di reato, ad esempio per certi illeciti finanziari o ambientali; non si denuncia perché non si ha fiducia nella giustizia, o addirittura perché si temono processi di vittimizzazione secondaria. Questo riguarda in particolare gruppi sociali marginalizzati, come migranti o minoranze razzializzate, più spesso oggetto di controllo che destinatari di protezione. Oppure, alcuni reati rimangono nascosti nel numero oscuro della criminalità per il potere sociale degli autori, mentre altri sono perseguiti a causa dell'allarme sociale che provocano, alimentato dai media, o per la facilità con cui determinati illeciti possono essere perseguiti. In questo quadro, alcuni reati – come quelli finanziari o ambientali – vengono raramente denunciati o perseguiti, mentre altri – ad esempio i reati di strada – sono registrati in quantità elevate dalle forze di polizia. Questo squilibrio alimenta il cosiddetto *base-rate problem*: la polizia raccoglie enormi quantità di dati, ma di qualità molto variabile e parziali. Tali database, già intrisi di *bias*, finiscono per trasferire questi stessi *bias* nei modelli predittivi. Si conferma così il principio del *garbage in, garbage out*: dati di scarsa qualità (*garbage in*) generano modelli fallaci (*garbage out*). Završnik, come altri autori, insiste sul carattere politico della produzione dei dati: qualcuno deve sempre decidere cosa rendere visibile, cosa proteggere e cosa interpretare[30].

Così come la costruzione di dataset in ambito penale non è un processo neutrale, nemmeno la costruzione di algoritmi lo è. Secondo Završnik, una volta costruiti, anche gli algoritmi riflettono le stesse dinamiche che abbiamo illustrato relativamente alla costruzione di dataset: i modelli riflettono valori e priorità che vanno resi espliciti.

[30] L. Gitelman (a cura di), *Raw Data Is an Oxymoron*, Cambridge (MA), MIT Press, 2013.

Benché da molte parti si invochi maggiore trasparenza, tale richiesta rischia di essere insufficiente. Infatti, tecniche come il machine learning e le reti neurali rimangono per loro natura delle *black boxes*, e sembra illusoria la richiesta di rendere questi processi algoritmici completamente spiegabili[31]. Facciamo chiarezza.

Le *reti neurali artificiali* sono modelli di calcolo ispirati al funzionamento del cervello umano. Sono composte da una serie di "nodi" o *neuroni artificiali* organizzati in livelli. Ogni nodo riceve dei dati, li elabora attraverso funzioni matematiche e li trasmette agli altri nodi. Attraverso un processo chiamato *apprendimento* (*training*), la rete modifica i "pesi" delle connessioni tra i nodi in base agli errori commessi, migliorando progressivamente le sue previsioni o classificazioni. Questo le rende particolarmente adatte a compiti complessi come il riconoscimento di immagini, la traduzione automatica o l'analisi predittiva. Sono però considerate *black boxes* perché, anche se si può osservare il risultato finale, è difficile capire in dettaglio come la rete sia arrivata a quell'output. Un esempio di rete neurale in giustizia penale potrebbe essere un algoritmo usato per prevedere la probabilità di recidiva di un imputato, uno strumento utilizzato più negli Stati Uniti che in Italia. Una rete neurale riceve come *input* variabili quali età, precedenti penali, quartiere di residenza, livello di istruzione, situazione lavorativa, ecc. Attraverso i suoi livelli di nodi, la rete combina questi dati in modi molto complessi e produce un *output* finale: ad esempio, "70% di probabilità che l'imputato commetta un nuovo reato entro 2 anni". Il problema è che, essendo una *black box*, è difficile spiegare al giudice (o all'imputato stesso) come la rete abbia pesato i diversi fattori per arrivare a quel 70%. Questo solleva questioni di trasparenza e di diritto alla difesa.

Per verificare eventuali discriminazioni risultano utili gli *audit esterni*[32]. Gli *audit esterni* sono controlli indipendenti condotti da soggetti terzi (non dagli stessi sviluppatori o utilizzatori dell'algoritmo) con l'obiettivo di valutare il funzionamento e gli effetti di un sistema algoritmico. Possono servire, ad esempio, a verificare se un algoritmo produce discriminazioni, se rispetta i principi di trasparenza e correttezza, o se funziona come dichiarato. L'idea è simile a quella della revisione contabile nelle aziende: un soggetto indipendente esamina procedure e risultati per aumentare la fiducia pubblica e garantire che il sistema non causi danni o violi diritti. Supponiamo che un tribunale utilizzi un algoritmo per stabilire la concessione della libertà vigilata. Alcuni studiosi o enti indipendenti (università, ONG, agenzie governative di garanzia dei diritti) potrebbero

[31] Anche se esistono studi e ricerche che lavorano sulla spiegabilita. Si veda M. Palmirani, *Big Data e conoscenza*, in *Rivista Italiana di Filosofia del diritto*, 2020, IX, 1, pp. 73-92.

[32] A. Završnik, *Algorithmic justice*, cit.

condurre un audit esterno per verificare se l'algoritmo tratta allo stesso modo imputati bianchi e imputati neri, o se penalizza sistematicamente chi vive in determinati quartieri. Un audit potrebbe scoprire, ad esempio, che il modello attribuisce un rischio molto alto a chi proviene da zone con alti tassi di criminalità, anche se l'individuo non ha una storia criminale significativa. In questo caso, l'audit servirebbe a dimostrare che l'algoritmo incorpora un *bias* geografico che funziona come un sostituto della razza[33].

Tuttavia, nemmeno gli audit sono in grado di risolvere ogni criticità. Završnik mette in guardia contro la tentazione di ridurre questioni complesse a semplici calcoli. Il nodo non si esaurisce nella richiesta di algoritmi "più trasparenti": la vera domanda è se tali strumenti contribuiscano davvero a migliorare la società. Si pensi, ad esempio, agli algoritmi che stimano il rischio di recidiva o la probabilità che un imputato si presenti al processo. Invece di concentrarsi esclusivamente su chi non si presenterà, sarebbe forse più utile indagare le cause sociali di tale comportamento: si tratta di difficoltà economiche che impediscono di comparire in giudizio? Della mancanza di mezzi di trasporto?[34] Porre questo tipo di domande significa adottare un approccio radicalmente diverso da quello che i database, da soli, sono in grado di offrire.

La costruzione di database e algoritmi in giustizia penale è tutt'altro che un processo tecnico e neutrale, ma rappresenta una pratica carica di scelte politiche e sociali, capace di consolidare rapporti di potere e di riprodurre disuguaglianze sistemiche sotto l'apparenza di neutralità scientifica.

3.3 Utilizzo dei big data nel sistema della giustizia penale

Per ragionare sulle implicazioni dell'utilizzo dei big data e del controllo *data driven* nel sistema della giustizia penale[35], sembra utile partire da un articolo seminale di Chan e Bennett Moses del 2016, pubblicato sulla rivista *Theoretical*

---

[33] B. E. Harcourt, *Risk as a Proxy for Race: The Dangers of Risk Assessment*, in *Federal Sentencing Reporter*, 2015, 27, pp. 237-243.

[34] R. Courtland, *Bias detectives: The researchers striving to make algorithms fair*, in *Nature*, 2018, 558(7710), pp. 357-360.

[35] Per lavori che si occupano di questa tematica dal punto di vista giuridico e della filosofia del diritto, si veda, ad esempio: G. Contissa, G. Lasagni, G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di Internet*, 2019, 4, pp. 619-634; G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, Giappichelli, 2022; G. Lasagni, G. Contissa, *Un approccio computabile ai diritti processuali penali e al principio del mutuo riconoscimento. I progetti di ricerca CrossJustice e FACILEX*, in *Diritto di Difesa*, 2025, 3-4, pp. 662-676; F. Galli, *L'analisi automatica delle decisioni giudiziali*, Torino, Giappichelli, 2025.

criminology. Un articolo molto influente e molto citato nella nascente criminologia digitale, intitolato *Is big data challenging criminology?*

L'articolo parte dalle provocazioni di Chris Anderson e di Mayer-Schönberger e Cukier. Secondo Anderson, l'avvento dell'era dei petabyte e degli algoritmi avrebbe reso obsoleto il metodo scientifico classico, che richiede di partire da un'ipotesi, testare tale ipotesi tramite la ricerca, ed elaborare una tesi che confermi o neghi l'ipotesi elaborata. Secondo Anderson, con i big data non c'è più bisogno di un'ipotesi, poiché i dati parlerebbero da soli. Inoltre, non c'è più bisogno di ricercare una relazione causale tra i fattori che possano individuare le cause che portano a un dato fenomeno, ma basta osservare che esiste una correlazione tra due fenomeni[36]. Mayer-Schönberger e Cukier rafforzano questa idea, affermando che i big data hanno trasformato radicalmente il modo di comprendere il mondo, rendendo superflua la ricerca delle relazioni causali tra due elementi e sufficiente l'individuazione di una semplice correlazione[37]. Nell'articolo, Chan e Bennett Moses esaminano criticamente tali affermazioni alla luce della pratica criminologica.

Le due autrici riflettono sull'uso che dei big data può fare la criminologia, come fonte per la ricerca criminologica o come strumento predittivo. Tratteremo dei big data come fonte per la ricerca criminologica nel prossimo paragrafo, per adesso ci soffermiamo sull'utilizzo dei big data come strumento predittivo.

Quella in chiave predittiva è l'applicazione più controversa dei big data nel sistema della giustizia penale. Si tratta dell'utilizzo di algoritmi per anticipare comportamenti criminali o supportare decisioni operative in ambito penale. Chan e Bennett Moses analizzano con particolare attenzione lo sviluppo del *predictive policing*, che si propone di identificare luoghi, momenti o individui a rischio sulla base di dati storici e correlazioni statistiche, seguendo approcci che si ispirano a teorie criminologiche come la prevenzione situazionale o la vittimizzazione ripetuta. La polizia predittiva verrà analizzata in dettaglio nel prossimo capitolo. Qui vogliamo soffermarci, invece, sul fatto che l'impiego di tecniche di *machine learning* (come le *random forests*) porta a prediligere la precisione predittiva a scapito della spiegazione causale. Ovvero: si preferisce rintracciare la correlazione tra due elementi senza che si consideri rilevante cercare di identificare come e perché i due elementi siano in correlazione tra loro. Le autrici mettono in guardia contro i rischi epistemologici e pratici di que-

[36] C. Anderson, *The end of theory: The data deluge makes the scientific method obsolete*, in *Wired Magazine*, 23 giugno 2008

[37] V. Mayer-Schönberger, K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, London, John Murray, 2013.

sto approccio: senza una comprensione dei meccanismi causali, le correlazioni possono produrre previsioni fuorvianti, instabili o autoreferenziali, soprattutto in presenza di effetti di retroazione (*feedback loops*) o *bias* nei dati. Proviamo a spiegare meglio.

Un punto centrale della critica sviluppata da Chan e Bennett Moses riguarda la pretesa che i big data rendano superflua la teoria nelle scienze sociali, rendendo possibile sostituire l'indagine causale con la mera identificazione di pattern e correlazioni. Le autrici contestano l'idea secondo cui l'analisi dei dati su larga scala permetta di «lasciare che i dati parlino da soli», spostando il focus dal "perché" al "cosa". In realtà, sostengono, ogni operazione analitica incorpora assunzioni teoriche, anche quando non esplicitate: dalla selezione delle variabili, alla definizione ontologica dei dati, fino alla scelta degli strumenti statistici e algoritmici. Non esiste una "neutralità" epistemica nella costruzione o interpretazione dei dati.

La correlazione non può essere sufficiente a generare conoscenza utile e oggettiva. Senza spiegazioni delle relazioni causali che legano due elementi in correlazione, quella correlazione risulta irrilevante sotto vari punti di vista. Senza teoria, osservano Chan e Bennett Moses, è impossibile comprendere quando le correlazioni siano valide, perché emergano, e quali effetti possa avere agire su di esse. Senza teoria, diventa impossibile valutare gli effetti delle decisioni basate sui dati. E senza spiegazione causale di una correlazione pur osservata tra due elementi, si finisce per ostacolare la possibilità di intervenire in quella correlazione. Per le autrici, la teoria non è solo uno strumento esplicativo, ma anche una guida epistemologica e normativa, fondamentale per garantire la coerenza, la giustificazione e la legittimità delle pratiche criminologiche nell'era del big data. Proviamo a riproporre un esempio per rendere più chiaro il punto.

Immaginiamo che l'analisi dei dati riveli un legame statistico, una correlazione, tra la misura delle scarpe di un detenuto e la probabilità di recidiva[38]. Seguendo una logica strettamente predittiva, la dimensione della scarpa potrebbe essere inclusa come variabile utile a stimare il rischio di ricommettere reato. Preso alla lettera, questo significherebbe che il numero di scarpe potrebbe essere usato come variabile predittiva nelle decisioni giudiziarie. Ma un simile legame non ha alcun senso causale: non sono certo i piedi grandi a spingere qualcuno a delinquere di nuovo. La correlazione potrebbe invece dipendere da cause nascoste, come ad esempio effetti istituzionali indiretti. Per fare un esempio estremo: se in passato le carceri avessero avuto difficoltà a reperire calzature di grandi numeri, i detenuti con piedi più grandi avrebbero potuto essere rilasciati prima.

[38] R. Berk, *Criminal Justice Forecasts of Risk: A Machine Learning Approach*, New York, Springer, 2012.

Se il tempo di detenzione è collegato ai tassi di recidiva (perché chi rimane più a lungo segue più programmi riabilitativi, oppure al contrario chi esce prima si reintegra meglio nella società), ecco che la misura delle scarpe apparirebbe legata al rischio di recidiva. Questo esempio rende evidente il problema: le correlazioni da sole non spiegano nulla. Senza una comprensione delle cause reali e dei meccanismi sociali che producono i dati, rischiamo di scambiare per predittori utili delle semplici coincidenze o degli artefatti statistici, con conseguenze arbitrarie e potenzialmente ingiuste nelle decisioni penali. Allora, un intervento produttivo di cambiamento, più che basare la decisione riguardo alla probabilità di recidiva sulla misura del piede, dovrebbe agire sulla mancanza di calzature adatte nelle carceri. In altre parole, prendere decisioni giudiziarie basandosi solo sulla correlazione produrrebbe conseguenze arbitrarie o ingiuste.

Questo esempio mostra bene perché, nel campo della giustizia penale, non basti "prevedere" tramite correlazioni: occorre interrogarsi sulle cause reali e sui meccanismi sociali che legano variabili e comportamenti, per evitare che l'analisi algoritmica diventi un esercizio sterile o discriminatorio.

Chan e Bennett Moses approfondiscono proprio i rischi epistemologici e operativi legati all'uso di modelli predittivi non causali.

Uno degli aspetti più problematici sollevati da Chan e Bennett Moses riguardo all'uso predittivo dei big data nel sistema della giustizia penale è il rischio di effetti di retroazione (*feedback loops*), ossia dinamiche per cui le previsioni generate dai dati influenzano il contesto stesso da cui i dati sono tratti, alterandone la validità futura. Un primo tipo di retroazione si verifica quando l'azione basata sulla previsione modifica il comportamento dei soggetti osservati. Ad esempio, se le forze di polizia concentrano la sorveglianza su individui o aree selezionate algoritmicamente, ciò può portare i potenziali trasgressori a cambiare le proprie strategie, eludendo i criteri predittivi senza necessariamente ridurre la propensione criminale. Un secondo, più insidioso, effetto di retroazione si manifesta nella distorsione della raccolta dati: l'intensificazione della presenza di polizia in certe zone aumenta la probabilità che crimini vengano rilevati in quei luoghi, generando un apparente incremento della criminalità che giustifica ulteriori interventi, alimentando un circolo vizioso. Questo può condurre a una perpetuazione di *bias* preesistenti, come la sorveglianza sproporzionata di minoranze o quartieri marginalizzati, rafforzando stereotipi e disuguaglianze sistemiche. Inoltre, le autrici evidenziano che questi fenomeni di retroazione non possono essere corretti semplicemente aggiornando i dati, poiché le assunzioni causali implicite negli algoritmi e nei sistemi di decisione restano inalterate. In assenza di una comprensione teorica dei meccanismi sociali coinvolti, l'uso dei big data rischia dunque di produrre conseguenze controintuitive o ingiustifica-

te, minando l'efficacia e la legittimità delle politiche di prevenzione e controllo del crimine.

Secondo Chan e Bennett Moses, i big data non sono di per sé una minaccia, ma lo diventa un uso acritico che ignora le teorie e i meccanismi causali. La criminologia non deve rifiutare i big data, ma integrarli in un approccio riflessivo, teoricamente informato. Le autrici auspicano che il ruolo della teoria rimanga centrale, specialmente per guidare interventi di politica criminale efficaci, equi e trasparenti. Sul ruolo dei big data nella criminologia torneremo a breve nel prossimo paragrafo.

Sul tema delle correlazioni, risultano particolarmente interessanti anche le riflessioni di Završnik. Egli osserva che gli algoritmi di valutazione del rischio operano producendo probabilità, ma non certezze, e soprattutto rilevano correlazioni senza poter stabilire relazioni causali[39]. In altre parole, indicano solo correlazioni statistiche (ad esempio: "questa persona ha il 60% di probabilità di recidiva"), ma non stabiliscono cause reali del comportamento criminale. Un algoritmo può trovare che età, precedenti penali o quartiere di residenza siano fortemente correlati con la recidiva, ma questo non significa che questi fattori *causino* direttamente il crimine. Il pericolo, secondo l'autore, è che queste correlazioni vengano reificate e utilizzate come basi decisive per limitare la libertà individuale, pur non avendo il valore esplicativo o giustificativo che normalmente richiederebbero i principi del diritto penale. Un algoritmo può stimare che un individuo abbia, ad esempio, il 60% di probabilità di recidiva, ma tale numero non significa che quel soggetto *causerà* necessariamente un reato: si tratta solo di una correlazione statistica ricavata da dati passati. Per questo motivo, le correlazioni devono sempre essere interpretate da un umano: è il giudice o il decisore che attribuisce significato ai numeri. Ma anche qui entra in gioco la politica: decidere se concedere la libertà vigilata a chi ha una probabilità del 40% di recidiva o negarla a chi ha l'80% non è una scelta "scientifica", è una scelta valoriale e politica legata al contesto sociale, economico e culturale[40]. Per esempio, in società con carceri sovraffollate la soglia di rischio accettabile può essere più bassa (cioè più liberazioni), mentre in contesti dominati da politiche securitarie o dall'influenza dell'industria carceraria la soglia può essere molto più alta (cioè più incarcerazioni).

Završnik nota che esistono metodi statistici più avanzati e richiama il lavoro di Marchant, che propone l'uso di metodi di ottimizzazione bayesiana[41]. Questi

[39] A. Završnik, *Algorithmic justice*, cit.

[40] *Ibidem*.

[41] R. Marchant, *Bayesian techniques for modelling and decision-making in criminology and social sciences*, presentazione alla conferenza *Automated Justice: Algorithms, Big Data and Criminal Justice Sys-*

consentono non solo di calcolare una probabilità, ma permettono di misurare anche il grado di "certezza" con cui un algoritmo stima una probabilità.

Nella probabilità semplice, quando un algoritmo calcola, ad esempio, che una persona ha il 60% di probabilità di recidiva, ci sta dando una stima puntuale. Ma quella percentuale è solo un numero "medio", ricavato da dati passati e da correlazioni statistiche. Non sappiamo *quanto* possiamo fidarci di quel numero: potrebbe essere basato su moltissimi casi simili (quindi relativamente solido) oppure su pochi dati rumorosi (quindi molto incerto). L'approccio bayesiano introduce un elemento in più: non solo fornisce una probabilità, ma anche una misura della certezza (o confidenza) associata a quella probabilità. Così, invece di affermare semplicemente che un imputato ha il 60% di probabilità di recidiva, un modello bayesiano specificherebbe, ad esempio, se tale valore è stimato con un'incertezza di ±5% (intervallo 55-65%) o con un'incertezza di ±25% (intervallo 35-85%). Nel primo caso, la previsione sarebbe relativamente solida; nel secondo, invece, l'algoritmo risulterebbe molto meno affidabile, lasciando un ampio margine di dubbio. Questo è utile perché permette al decisore (giudice, commissione di libertà vigilata, ecc.) di capire non solo la stima del rischio, ma anche quanto l'algoritmo è sicuro di quella stima. Un sistema di ottimizzazione bayesiana permette quindi di confrontare non solo i valori medi (60%), ma anche la loro affidabilità.

Tuttavia, per Završnik, questa distinzione mette in luce un punto fondamentale: anche laddove si introducano tecniche statistiche più raffinate, permane il problema di decidere quanta incertezza sia accettabile come base per una decisione che incide direttamente sulla libertà personale. Di conseguenza, il ricorso a tali strumenti non elimina ma anzi rende più evidente la dimensione politica e discrezionale delle scelte giudiziarie, mostrando come il linguaggio matematico non possa sostituire il dibattito normativo e democratico sulle soglie di rischio tollerabili. E il dibattito normativo e democratico, accademico e pubblico, intorno all'utilizzo dei big data nel sistema della giustizia penale è fondamentale.

Qui sembra interessante riportare una riflessione di Hanna-Moffatt in merito alla giustizia algoritmica. La studiosa punta infatti l'attenzione, in maniera parecchio originale, al potenziale uso attivista dei big data, intesi come strumenti per smascherare le pretese di neutralità delle tecnologie predittive[42]. In questa prospettiva, l'autrice richiama una inchiesta di *ProPublica* sul sistema COM-

tems, Collegium Helveticum, Zürich, 20 aprile 2018, disponibile su: https://collegium.ethz.ch/wp-content/uploads/2018/01/180420_automated_justice.pdf.

[42] K. Hannah-Moffat, *Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates*, in *Theoretical Criminology*, 2018, 23(4), pp. 453-470.

PAS, utilizzato in numerosi tribunali statunitensi per valutare la probabilità di recidiva[43].

ProPublica è una redazione giornalistica investigativa indipendente e senza scopo di lucro, fondata tra il 2007 e il 2008. ProPublica è citata per aver condotto la celebre inchiesta "*Machine Bias*". Il lavoro ha analizzato COMPAS, un software di valutazione del rischio di recidiva usato nei tribunali statunitensi, mostrando come l'algoritmo producesse stime sistematicamente distorte: tendeva a sovrastimare il rischio di recidiva per gli imputati afroamericani e a sottostimarlo per gli imputati bianchi, pur in presenza di comportamenti successivi opposti. Hannah-Moffat definisce questa inchiesta un esempio di lavoro collettivo perché non è frutto di un solo giornalista, ma è il risultato della cooperazione tra più reporter interni, analisti e il team di data journalism di ProPublica. Inoltre, la scelta di rendere pubblici i dati e i metodi usati nella ricerca ha favorito un confronto aperto: accademici, operatori del diritto penale, statistici e organi di critica hanno risposto con analisi e repliche, generando un ampio dibattito, pubblico e accademico, sulla correttezza e neutralità degli algoritmi di *risk assesment*. In particolare, la società produttrice, Northpointe (oggi Equivant), ha contestato i risultati, sostenendo che le metriche utilizzate da ProPublica fossero fuorvianti e che l'algoritmo fosse accurato secondo altre definizioni di equità. La controversia ha messo in luce un problema tecnico cruciale: diverse nozioni di *fairness* possono produrre risultati incompatibili. ProPublica aveva adottato come criterio principale la riduzione dei *false positive* (ossia i casi in cui un individuo veniva classificato ad alto rischio senza poi recidivare), mentre Northpointe difendeva il principio di *predictive parity* (la corrispondenza tra la probabilità predetta e i risultati effettivi). Entrambe le metriche sono statisticamente valide, ma non possono essere soddisfatte contemporaneamente: un algoritmo che bilancia un criterio tende inevitabilmente a sacrificare l'altro. Questa discussione ha mostrato che il problema non riguarda soltanto la programmazione dei modelli, ma anche la costruzione e la selezione dei database utilizzati: se i dati di partenza riflettono pratiche di polizia razzializzate o disuguaglianze sistemiche, l'algoritmo finisce per riprodurre e rafforzare tali distorsioni, indipendentemente dal criterio di equità scelto. In questo senso, l'inchiesta di ProPublica ha favorito un confronto informato non solo sugli algoritmi, ma anche sulla qualità e sul significato politico dei dati che ne costituiscono la base, aprendo spazi di discussione che coinvolgono tanto giuristi e informatici quanto attivisti e giornalisti investigativi. Per Hannah-Moffat, questo episodio rappresenta un

[43] ProPublica, *COMPAS recidivism risk score data and analysis*, 2017, https://www.propublica.org/datastore/dataset/compas-recidivism-risk-score-dataand-analysis.

esempio paradigmatico di come dataset pubblici e analisi indipendenti possano essere mobilitati in chiave critica, generando una forma di *information activism* che mette in discussione la legittimità politica e morale degli algoritmi di *risk assessment*. In tal senso, Hannah-Moffatt evidenzia la dimensione conflittuale e contestabile delle tecnologie predittive: esse non sono solo strumenti di governance, ma anche oggetto di pratiche di resistenza e contro-narrazione che ne rivelano il carattere discriminatorio e ne contestano l'uso nelle decisioni giudiziarie.

Il punto però è che tra i tecno-ottimisti dell'utilizzo delle tecnologie *data-driven* nel sistema della giustizia penale c'è anche l'idea che queste tecnologie possano essere utili per affrontare il problema dei pregiudizi nei processi decisionali.

Završnik si domanda se sia preferibile affidarsi al giudizio umano, spesso influenzato da stereotipi, o a sistemi algoritmici che promettono neutralità[44]. L'autore ricorda che numerose ricerche hanno mostrato quanto le decisioni giudiziarie siano esposte a fattori contingenti e irrazionali: ad esempio, uno studio di Danziger, Levav e Avnaim-Pesso ha dimostrato che i giudici tendono a negare più frequentemente la libertà vigilata verso la fine delle sessioni e ad essere più indulgenti subito dopo una pausa o un pasto[45]. In questo contesto, gli algoritmi potrebbero apparire come una soluzione per eliminare l'arbitrarietà. Tuttavia, Završnik – come tanti altri che abbiamo già visto e che continueremo a vedere – evidenzia come anche i sistemi automatici siano inevitabilmente portatori di *bias*, poiché vengono "nutriti" con dati sociali e culturali che incorporano già serie storiche di disuguaglianze. Perfino concetti statistici apparentemente neutri, come medie, deviazioni standard o regressioni, sono il risultato di processi culturali e storici[46].

Završnik utilizza questa osservazione per mostrare che quando tali strumenti vengono applicati alla giustizia penale non possono essere considerati "puri calcoli": essi portano con sé un bagaglio culturale e storico che condiziona le decisioni algoritmiche tanto quanto condiziona quelle umane. Ad esempio, scegliere di trattare persone e comportamenti attraverso categorie statistiche "equivalenti" (come gruppi di rischio) implica un atto di riduzione e normalizzazione

---

44 A. Završnik, *Algorithmic justice*, cit.

45 S. Danziger, J. Levav, L. Avnaim-Pesso, *Extraneous factors in judicial decisions*, in *Proceedings of the National Academy of Sciences*, 2011, 108(17), pp. 6889-6892.

46 A. Desrosières, *The Politics of Large Numbers: A History of Statistical Reasoning*, Cambridge (MA), Harvard University Press, 2002; S. Brayne, *Big Data Surveillance: The Case of Policing*, in *American Sociological Review*, 2017, 8,1, pp. 977-1008; A. Meijer, M. Wessels, *Predictive Policing: Review of Benefits and Drawbacks*, in *International Journal of Public Administration*, 2019, 42(12), pp. 1031-1039.

che nasce da visioni culturali precise di cosa sia comparabile e di cosa non lo sia. Anche concetti apparentemente neutri come la *regressione* si basano sull'idea che si possano prevedere comportamenti futuri sulla base di regolarità passate: ma questa idea, applicata alla criminalità, rischia di trasformarsi in un meccanismo che cristallizza e riproduce le disuguaglianze sociali già presenti nei dati storici.

In questo senso, l'autore ribadisce che il problema dei *bias* non può essere ridotto a un errore tecnico o a un difetto dei programmatori: esso è strutturale, perché riguarda la natura stessa della matematica applicata al sociale. Gli algoritmi "ereditano" questo carattere culturale e storico delle categorie statistiche, e quindi non possono mai essere davvero neutrali. In altre parole, anche gli strumenti matematici che oggi consideriamo universali sono il risultato di decisioni, interpretazioni e mediazioni che riflettono valori e priorità di specifici contesti sociali. Ad esempio, questo vale anche per uno studio che ha analizzato i modelli di linguaggio utilizzati per addestrare le intelligenze artificiali, dimostrando che queste ultime, proprio attraverso il linguaggio, assorbano inevitabilmente i pregiudizi presenti nella società[47]: i sistemi di apprendimento automatico finiscono quindi per riprodurre, e talvolta amplificare, discriminazioni preesistenti.

Si pone allora un duplice dilemma, che entra in dialogo anche con le riflessioni di Hanna-Moffatt sopra esposte: da un lato, risulta urgente chiedersi se sia possibile e desiderabile "ripulire" i dati da questi pregiudizi (con il rischio di un'illusoria "neutralità" che li riproduce comunque attraverso *proxy*); dall'altro, se sia auspicabile affidare decisioni politiche e normative a ingegneri informatici che operano dietro porte chiuse. Infatti, così facendo, mancherebbe quel confronto pubblico (e quindi il controllo democratico) sulla giustizia algoritmica più volte richiamato[48]. Per Završnik, i codici costituzionali e le procedure penali, pur imperfetti, rappresentano il frutto di processi democratici, mentre un'operazione di *de-biasing* condotta in laboratorio rischierebbe di spostare il potere decisionale a un'élite tecnica. La domanda finale diventa dunque se sia preferibile convivere con i limiti e i pregiudizi umani, che includono anche empatia e intelligenza emotiva, o affidarsi a sistemi automatizzati che promettono oggettività ma rischiano di cancellare proprio quelle qualità umane che rendono possibile una giustizia sensibile ai contesti e ai bisogni delle persone.

---

47 A. Caliskan, J.J. Bryson, A. Narayanan, *Semantics derived automatically from language corpora contain human-like biases*, in *Science*, 2017, 356(6334), pp. 183-186.

48 K. Hannah-Moffat, *Algorithmic risk governance*, cit.; J. Chan, L. Bennett Moses, *Is Big Data challenging criminology?*, cit.; S. Milivojevic, *Crime and Punishment in the Future Internet*, cit.

E questo ci porta a un'ultima riflessione proprio sul diritto e sull'importanza della decisione umana nel procedimento giuridico.

Završnik analizza la logica degli algoritmi auto-apprendenti e i rischi che essa comporta per il diritto penale. I sostenitori dei modelli di *reinforcement learning* affermano che basti avere pazienza: algoritmi sempre più "intelligenti", corretti continuamente grazie a meccanismi di ricompensa e punizione, sarebbero in grado di migliorarsi all'infinito e di superare gli attuali difetti. Questa visione, però, per Završnik rivela l'ideologia del big data: un atteggiamento apologetico che invita ad attendere la perfezione futura della tecnologia, anziché riconoscere i limiti intrinseci della vita sociale, sempre troppo complessa per essere completamente formalizzata.

Il problema principale è che gli algoritmi rischiano di rimanere intrappolati in circuiti decisionali autoreferenziali, che riproducono all'infinito la logica incorporata nei dati di partenza. Diversamente, l'evoluzione giuridica si fonda storicamente sulla capacità di attribuire peso a circostanze nuove e di trasformare le regole precedenti attraverso la creazione di precedenti innovativi. Se gli algoritmi si basano unicamente sul rafforzamento di regole passate, le nuove situazioni rischiano di non trovare spazio e il diritto di smettere di evolvere[49].

Završnik avverte quindi che la logica circolare dei modelli auto-apprendenti può congelare l'interpretazione giuridica, impedendo l'adattamento delle norme ai mutamenti sociali e culturali. Il risultato sarebbe un sistema di "giustizia automatizzata" che consolida il passato, ma non è in grado di rispondere al presente né di generare nuove traiettorie per il futuro.

Il rischio insito in una giustizia automatizzata (*automated justice*) è che, se gli algoritmi auto-apprendenti funzionano attraverso cicli di retroazione continua (*feedback loops*), le decisioni si basano sempre su regole già consolidate e sugli schemi del passato.

In questo modo, la giustizia automatizzata tende a riprodurre all'infinito logiche e pregiudizi incorporati nei dati, impedire che nuovi casi possano trasformarsi in precedenti innovativi, che storicamente sono stati il motore dell'evoluzione giuridica, e congelare così l'interpretazione del diritto, consolidando l'"eterno passato" invece di adattarsi al presente. Završnik mette in guardia da questa dinamica: se la giustizia diventa pienamente automatizzata, si rischia di sacrificare proprio quella capacità creativa e adattiva che rende il diritto uno strumento vivo e capace di evolversi con la società.

[49] A. Završnik, *Algorithmic justice*, cit.

3.4 Utilizzo dei big data in criminologia

Come sottolineano Aragona e Stefanizzi, nella società digitale si assiste sempre più alla crescente traduzione delle interazioni sociali in dati digitali e questo pone delle sfide alla ricerca sociologica, che deve innovare sia le tecniche sia le domande di ricerca. Infatti, sono necessarie tecniche nuove adatte a indagare interazioni sociali oggettificate in dati, per rispondere a domande nuove che problematizzino e interroghino «i processi che danno forma alla produzione di numeri» che, a loro volta, possono modificare la realtà sociale. La ricerca sociologica dovrebbe comprendere come e quando ciò possa avvenire[50].

Dunque, studiare le interazioni nella società digitale, dove tutto (o quasi) avviene in compresenza tra digitale e sociale, dove tutta una serie di interazioni si sono spostate dallo spazio reale al cyberspazio ma continuando ad avere effetti sul reale, la sociologia deve confrontarsi con sfide nuove. Deve prestare attenzione a quanto avviene nel mondo digitale, alle ripercussioni nel mondo reale di ciò che avviene nel mondo digitale, ma anche al ruolo che il mondo reale ha nel determinare le condizioni delle interazioni che avvengono nel mondo digitale. Dunque, per riuscire a muoversi in quel terreno in cui digitale e reale sono costantemente in compresenza, la sociologia deve non solo innovare le proprie domande e tecniche di ricerca, ma deve anche rafforzare le conoscenze di base in altri campi del sapere, come l'informatica, la matematica, le *computer sciences*. Per la criminologia, che di base è una scienza sociale e dunque viene investita da questa "*data revolution*"[51] tanto quanto le scienze sociali più in generale, questo passaggio potrebbe essere meno problematico, essendo per sua natura interdisciplinare[52].

Nel contesto criminologico, l'uso dei big data come fonte per la ricerca criminologica significa principalmente integrare nelle pratiche di ricerca esistenti nuove tipologie di dati digitali, come quelli provenienti dai social media o dalle telecomunicazioni. In questa forma, il big data non costituisce una rottura epistemologica, ma rappresenta un'estensione delle metodologie tradizionali[53]. Proponiamo alcuni esempi che illustrino questo genere di utilizzo dei big data.

Per indagare il ruolo dei social media durante proteste e disordini di piazza, alcuni studi analizzano milioni di tweet applicando metodi simili a quelli della *content analysis* classica, sebbene su scala ampliata. Il vantaggio è quello di poter

50 B. Aragona, S. Stefanizzi, *Società digitale: interrogativi, aree di ricerca e ruolo della sociologia*, cit.
51 R. Kitchin, *The Data Revolution*, cit.
52 M. Bosworth, C. Hoyle (a cura di), *What is criminology?*, Oxford: Oxford University Press.
53 J. Chan, L. Bennett Moses, *Is Big Data challenging criminology?*, cit.

accedere facilmente a una quantità di dati impressionante, su scala molto più ampia rispetto a quanto si potesse fare analizzando solo comunicati, volantini, interviste qualitative, articoli di giornale. Tuttavia, è importante che chi analizza questi dati tenga conto della loro parzialità intrinseca. Ad esempio, possono esistere dei *bias* negli *hashtag* e non è possibile accedere ai messaggi privati. Inoltre, va considerato il *divide* tecnologico, compreso il fatto che, a causa dell'accesso differenziale alle tecnologie, potrebbero mancare delle variabili demografiche fondamentali.

Altri studi analizzano la correlazione tra presenza umana e crimine urbano utilizzando i dati delle telecomunicazioni e quelli delle denunce. L'utilizzo dei dati aggregati provenienti da operatori telefonici per mappare la mobilità urbana e correlarla con i tassi di criminalità si iscrive entro il paradigma quantitativo già consolidato nella disciplina. Tuttavia, i dati presi in analisi, nonostante la grande mole, soffrono di limiti importanti in quanto a rappresentatività del campione. Ad esempio, i ricercatori in questo caso erano riusciti ad accedere ai dati delle telecomunicazioni di un grande operatore telefonico. Circa il 25% della popolazione si avvale di tale operatore. L'analisi deve tenere conto di questo limite nel ragionare intorno alle correlazioni che possono emergere. Dall'altro lato, anche il crimine urbano registrato nell'area non rappresenta, lo abbiamo visto, la misura reale della criminalità.

Utilizzando questi esempi, Chan e Bennett Moses spiegano che i big data pongono interrogativi importanti riguardo alla qualità, alla rappresentatività e all'accessibilità delle informazioni. Esiste un'illusione diffusa associata ai big data, ovvero la convinzione che si possa ottenere una rappresentazione della realtà esaustiva e priva di distorsioni. In altre parole, per prendere in prestito le parole di Mayer-Schönberger e Cukier, nell'era digitale in cui i big data sono la «rivoluzione che cambierà il modo in cui viviamo, lavoriamo e pensiamo», i processi di datificazione influenzeranno anche il nostro modo di fare ricerca. Ciò diventerà evidente in tre principali cambiamenti: 1) la necessità di formare gruppi di campionamento per la ricerca è un ricordo del passato poiché i big data ci forniscono sempre più accesso a tutte le informazioni in modo che N, la dimensione del campione, finisca per essere uguale a tutti (N=tutti); 2) l'accuratezza dei dati non è più qualcosa di cui preoccuparsi; 3) non c'è più bisogno di indagare sulle domande delle relazioni causali, poiché la correlazione da sola è sufficiente per generare conoscenza[54]. Mayer-Schönberger e Cukier sostengono che i sociologi perderanno il monopolio dell'analisi delle dinamiche sociali a causa di "N=tutti" e dovranno competere con informatici ed esperti di scienze

[54] V. Mayer-Schönberger, K. Cukier, *Big Data*, cit.

del computer. Tuttavia, gli esempi che abbiamo illustrato poc'anzi mostrano che esistono dei limiti e, nonostante la dimensione innovativa dei big data, il rigore metodologico e la riflessione teorica rimangono imprescindibili. Come abbiamo visto negli esempi precedenti, N non può includere tutti, né possiamo dare per scontato che il dato sia accurato.

Un altro elemento degno di riflessione per quanto riguarda l'utilizzo dei big data nell'indagine criminologica è la differente possibilità di accedere ai dati da parte di chi fa ricerca. Infatti, non tutti i ricercatori o attori sociali hanno lo stesso accesso ai dati[55].

In particolare, le grandi piattaforme tecnologiche (come Google, Facebook, Amazon) dispongono di enormi volumi di dati e delle risorse per analizzarli. Questo privilegio posiziona i cosiddetti "*data scientists*" in una posizione di potere rispetto agli accademici tradizionali, che spesso non hanno accesso a questi dati. Nella ricerca criminologica, l'accesso ai dati non è affatto garantito. Inoltre, la difficoltà di accedere ai dati "grezzi" o di capire i meccanismi interni degli algoritmi utilizzati (il cosiddetto *black box*) diventa una barriera all'inclusività e alla trasparenza del sapere scientifico.

Dunque, le asimmetrie nell'accesso ai dati e agli strumenti analitici influenzano chi può produrre conoscenza e in che modo, perpetrando squilibri di potere tra attori accademici, industriali e istituzionali.

Risulta utile richiamare a questo punto il concetto di capitale digitale.

Il concetto di *capitale digitale*, mutuato da Van Dijk e ispirato alla teoria del capitale di Bourdieu, è impiegato da Lavorgna e Ugwudike per descrivere le risorse (competenze tecniche, accesso ai dati, capacità di sviluppo tecnologico) che permettono ad alcuni attori di dominare la progettazione e l'implementazione delle tecnologie data-driven nella giustizia penale[56]. Lavorgna e Ugwudike evidenziano come questo capitale sia concentrato in mani privilegiate – come quelle di ricercatori in informatica, sviluppatori e grandi aziende – che detengono il potere di influenzare la progettazione degli algoritmi e le relative narrazioni. Al contrario, i gruppi socio-economicamente marginali, come minoranze etniche o persone con disabilità, risultano esclusi dalla partecipazione attiva allo sviluppo tecnologico, ma sono spesso i più esposti ai rischi di sorveglianza e pro-

---

55 D. BOYD, K. CRAWFORD, *Critical questions for Big Data*, cit.

56 P. BOURDIEU, *The forms of capital*, in J.G. RICHARDSON (a cura di), *Handbook of Theory and Research for the Sociology of Education*, Westport, Greenwood Press, 1986, pp. 241-258; J. VAN DIJK, *The Deepening Divide: Inequality in the Information Society*, Thousand Oaks, Sage, 2005; A. LAVORGNA, P. UGWUDIKE, *The datafication revolution in criminal justice: An empirical exploration of frames portraying data-driven technologies for crime prevention and control*, in *Big Data and Society*, 2021, 8(2).

filazione algoritmica[57]. L'asimmetria nella distribuzione del capitale digitale si traduce così in una distribuzione diseguale dei benefici e dei danni della *datification*, rendendo ancora più urgente un'analisi critica della governance tecnologica e della giustizia algoritmica.

L'accesso ai dati per fare ricerca è reso difficile dalla digitalizzazione. Il sapere sociologico non è più centrale nelle analisi dell'interazione sociale contemporanea, che, essendo in gran parte datificata, ha bisogno anche di altri saperi. Per questi stessi motivi, il sapere criminologico stesso sembra aver perso centralità anche nelle analisi del controllo e della criminalità nella società digitale. Il problema è che tale perdita di centralità ha delle ripercussioni importanti anche nei termini delle risposte elaborate in questi campi. Il sapere criminologico ha elaborato delle riflessioni per ciò che concerne la prevenzione da possibili abusi di potere da parte delle agenzie del controllo e di protezione dei diritti degli individui nel campo della giustizia penale. Questo tipo di riflessioni mancano invece nelle altre discipline, più attente a elaborare metodi per utilizzare i big data allo scopo di predire, sorvegliare, investigare. Si tratta del problema dello sfumare dei confini di regolazione, come scrive bene Završnik:

> Un altro aspetto cruciale dell'uso dei Big Data nel controllo della criminalità è il progressivo offuscamento dei confini normativi. Il nuovo linguaggio matematico si presta bene agli scopi della sicurezza (Amoore, 2014). In questo scenario, vengono inventati nuovi concetti sia per comprendere il crimine (produzione di conoscenza), sia per intervenire su di esso (politiche di controllo del crimine). Tra questi figurano *meaning extraction* (estrazione di significato), *sentiment analysis* (analisi del sentimento) e *opinion mining* (estrazione delle opinioni). Tuttavia, tali nozioni finiscono per indebolire le tradizionali linee di demarcazione nel dominio del controllo della criminalità: invece delle categorie relativamente ben definite del diritto penale – come sospetto, ragionevole dubbio, ecc. – che fungono da regolatori e da soglie all'intervento delle forze dell'ordine, i nuovi concetti non garantiscono più un adeguato contenimento delle agenzie né prevengono il rischio di abusi di potere[58].

---

[57] J. Van Dijk, *Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology*, in *Surveillance & Society*, 2014, 12(2), pp. 197-208; A. Willoughby, M. Nellis, *"You cannot really hide": Experiences of probation officers and young offenders with GPS tracking in Winnipeg, Canada*, in *Journal of Technology in Human Services*, 2016, 34(1), pp. 63-81.

[58] A. Završnik, *Big Data*, in M. Kaufmann, H.M. Lomell (a cura di), *De Gruyter Handbook of Digital Criminology*, Berlin-Boston, De Gruyter, 2025, pp. 107-114, p. 111.

Ovvero, nuovi concetti vengono utilizzati per capire la criminalità e per elaborare modelli di gestione della stessa (e sempre di più della sua prevenzione). Tuttavia, questi concetti non sono criminologici, non si sono formati in decenni di studi, riflessione, dibattito accademico, pubblico politico sulla criminalità e sul controllo, non tengono conto di tutti quei problemi teorici, metodologici e politici affrontati nella disciplina sin dagli albori a inizio Ottocento. E così, le nuove discipline scientifiche che stanno guadagnando terreno nell'analisi della criminalità nella società digitale, falliscono nell'obiettivo principale degli studi criminologici che, accanto al fatto di trovare una maniera per gestire e prevenire la criminalità, riflette sugli strumenti con cui raggiungere questo obiettivo. Strumenti che devono tenere in conto la protezione dei diritti degli individui e limitare l'abuso di potere da parte delle agenzie del controllo.

Vale la pena precisare, però, che non tutti gli studi contemporanei sull'utilizzo dei big data e della tecnologia più in generale in criminologia condividono uno stesso approccio. Purtroppo, mancano analisi critiche sui frame che supportano e diffondono queste tecnologie, con poche eccezioni. Nel loro interessante studio, Lavorgna e Ugwudike hanno identificato tre cornici principali entro cui i discorsi accademici tendono a rappresentare le tecnologie data-driven per la prevenzione e il controllo del crimine[59]. Esistono cornici ottimistiche, neutrali e oppositive. Queste cornici interpretative non sono altro che *immaginari sociotecnici* (*sociotechnical imaginaries*), ovvero «visioni collettive e performative di futuri desiderabili, animate da una comprensione condivisa delle forme di vita sociale e ordine sociale che si ritengono realizzabili grazie al progresso scientifico e tecnologico»[60]. Questi immaginari giocano un ruolo cruciale nella legittimazione delle tecnologie data-driven nel sistema di giustizia penale, promuovendole come strumenti neutrali, efficienti e inevitabili per il controllo del crimine. Secondo Lavorgna e Ugwudike, tali narrazioni utopiche contribuiscono a oscurare i danni sociali legati alla *datafication*, come la riproduzione di disuguaglianze storiche o la sorveglianza intrusiva. Gli immaginari sociotecnici, inoltre, influenzano non solo gli sviluppatori e le autorità pubbliche, ma anche la percezione dell'opinione pubblica, modellando le aspettative collettive rispet-

[59] Lo studio è basato su una revisione narrativa di 493 abstract accademici pubblicati tra il 2009 e il 2019, selezionati da Web of Science. Gli abstract sono stati codificati con l'ausilio di NVivo, classificando atteggiamenti, contesti disciplinari, ambiti di applicazione, e sviluppo tecnologico.

[60] S. Jasanoff, *Future imperfect: Science, technology, and the imaginations of modernity*, in S. Jasanoff, S.-H. Kim (a cura di), *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*, Chicago, University of Chicago Press, 2015, p. 25; vedi anche S. Jasanoff, S.-H. Kim, S. Sperling, *Sociotechnical Imaginaries and Science and Technology Policy: A Cross-National Comparison*, 2007, disponibile su: https://stsprogram.org/admin/files/imaginaries/NSF-imaginaries-proposal.pdf.

to al futuro della giustizia "intelligente". Tuttavia, proprio perché organizzano la conoscenza e strutturano il modo in cui pensiamo alle tecnologie[61], vanno sottoposti a scrutinio critico. Gli immaginari sociotecnici possono infatti alimentare visioni idealizzate che marginalizzano le preoccupazioni etiche e sociali a favore dell'efficienza.

Dalla ricerca di Lavorgna e Ugwudike emerge che gli studi che adottano frame ottimistici sono i prevalenti nel campo. Questi studi hanno una visione quasi utopica della tecnologia, specialmente del ruolo che svolge nel controllo del crimine, che è eccessivamente ottimista e si basa sul *techno-solutionism*. Essi descrivono le tecnologie come scientificamente oggettive, di gran lunga superiori alle capacità umane e indispensabili. Mettono in evidenza la loro capacità di migliorare l'efficacia della polizia, riducendone i costi e aumentandone l'efficienza amministrativa. Tuttavia, spesso trascurano i rischi associati all'utilizzo delle tecnologie digitali nelle pratiche di polizia, come i *bias* sistemici e le numerose altre violazioni non regolate. Altri studi adottano cornici neutre e, in questo caso, sono ambivalenti nell'atteggiamento, riconoscendo sia le conseguenze positive che negative dell'applicazione della tecnologia nel campo della giustizia penale. Alcuni sono informativi nel senso di richiedere una maggiore indipendenza nella ricerca e più trasparenza. Altri sono soluzionisti nel senso che riconoscono l'esistenza di problemi ma propongono soluzioni tecniche (es. modelli AI più equi). Ma gli studi che rientrano in questo approccio mancano di una seria critica strutturale e, in assenza di profonde riforme strutturali, propongono mere ottimizzazioni. Gli studi che adottano cornici oppositive rifiutano l'idea che la soluzione a tutto siano le tecnologie data-driven. Sono i meno numerosi ma anche i più ricchi da un punto di vista teorico. I *frame oppositivi* identificati da Lavorgna e Ugwudike mettono in luce una serie articolata di rischi sociali, legali ed etici legati all'applicazione delle tecnologie data-driven nel sistema di giustizia penale. Uno dei rischi più evidenti riguarda la violazione della privacy associata alla raccolta, conservazione e utilizzo non consensuale dei dati personali, spesso in contesti di sorveglianza invasiva e centralizzazione di database. Un altro rischio evidente è il pregiudizio razziale: l'uso di dati amministrativi storicamente distorti – come quelli sugli arresti – può portare a decisioni algoritmiche discriminatorie, generando un circolo vizioso di criminalizzazione di comunità già emarginate. I frame oppositivi criticano anche l'opacità algoritmica (*black-boxing*), che aumenta la difficoltà a contestare, addirittura compren-

[61] R.M. Entman, *Framing: Towards clarification of a fractured paradigm*, in *Journal of Communication*, 1993, 43, pp. 51-58; P. Borah, *Conceptual issues in framing theory: A systematic examination of a decade's literature*, in *Journal of Communication*, 2011, 61(2), pp. 246-263.

dere, le decisioni automatizzate, mettendo quindi in pericolo il diritto al giusto processo e l'*accountability*. Altri rischi includono la mancanza di regolamentazione adeguata, la mercificazione della giustizia penale (con aziende private che influenzano politiche pubbliche) e, più in generale, il consolidamento di *bias* sistemici che rafforzano disuguaglianze sociali strutturali. Questi *frame* si distinguono dagli altri per un approccio teorico più consapevole e critico, spesso radicato in discipline come la criminologia, il diritto e le scienze sociali e sono guidati da un'attenzione marcata per i diritti umani e la giustizia sociale.

Come emerso nell'analisi di Lavorgna e Ugwudike, l'adozione diffusa e non critica delle tecnologie data-driven nella giustizia penale ha implicazioni profonde che si articolano su due piani principali: sociale e politico. Sul piano sociale, l'espansione della *datafication* perpetua forme di danno algoritmico, in particolare per comunità già vulnerabili, come minoranze etniche e gruppi svantaggiati dal punto di vista socioeconomico. Questi danni includono sorveglianza discriminatoria, categorizzazioni impreviste e decisioni automatizzate basate su dati distorti, che rafforzano disuguaglianze storiche e consolidano narrazioni stigmatizzanti. Inoltre, affidarsi sempre più a strumenti percepiti come "oggettivi" rischia di sminuire l'importanza del giudizio umano, riducendo il margine di discrezionalità e la possibilità di riflessione critica caso per caso da parte degli operatori della giustizia. Sul piano politico, è possibile osservare come le logiche tecnocratiche e di controllo diventano prioritarie a discapito di valori democratici come trasparenza, accountability e giustizia procedurale. L'egemonia dei frame ottimistici, sostenuti da attori con elevato capitale digitale, ha facilitato la creazione e diffusione di strumenti che mirano all'efficienza, ma che trascurano le implicazioni etico-sociali del loro impiego. Inoltre, l'influenza di queste narrazioni rischia di legittimare un'espansione non regolata delle tecnologie, incentivando investimenti e politiche pubbliche orientate più all'innovazione tecnica che alla riflessione critica.

Lo studio mette in luce una diffusione sproporzionata dei frame ottimistici nelle ricerche che si occupano di tecnologie di controllo *data-driven*, il cui effetto è quello di guidare le politiche pubbliche e lo sviluppo di sistemi di giustizia automatizzati all'insegna di una *datafication* cieca ai rischi sociali e democratici.

Anche in criminologia è necessaria un'azione interdisciplinare e più inclusiva, che dia voce a prospettive finora marginalizzate e che favorisca una governance più equa e responsabile delle tecnologie nel sistema penale.

3.5 La performatività dei big data

Una delle questioni più complesse che emergono negli studi critici sui big data è la consapevolezza che i dati non descrivono la realtà in maniera oggettiva e imparziale[62], ma «agiscono su ciò che descrivono e retroagiscono su chi li utilizza e li costruisce». Essi partecipano alla costruzione di quella stessa realtà che pretendono semplicemente di descrivere. La quantificazione ha effetti performativi e trasformativi della realtà[63].

Nel dire che i dati sono performativi, Aragona e Stefanizzi si rifanno alla filosofia linguistica[64], in base alla quale è possibile creare cose con le parole. L'esempio classico è quello del matrimonio: nell'atto del dire "vi dichiaro marito e moglie", se le parole vengono pronunciate in un certo contesto, in un certo momento, e da chi ha l'autorità per pronunciarle, allora quelle parole sono in grado di creare cose. Le parole "vi dichiaro marito e moglie" producono davvero un legame matrimoniale, che diventa una cosa, con implicazioni precise ed effetti concreti e tangibili. In questo senso le parole sarebbero performative. La filosofa femminista Judith Butler ha ripreso il concetto della performatività in relazione al genere[65]. In questo caso, l'esempio classico è il momento in cui, alla nascita, il medico pronuncia la frase "è una bambina!" o "è un bambino!". Secondo Butler, questo è il primo atto attraverso cui il genere viene performato. Il genere è quindi, in questo senso, l'esito finale di una serie di atti, qualcosa che si fa, non una caratteristica di qualcuno che ne definisce l'identità. Il genere dunque come *performance*. La criminologa statunitense Nancy Wonders ha invece applicato il concetto di performatività ai confini[66]. In questo senso, i confini non sono i limiti geopolitici di un'unità territoriale, ma sono costruiti socialmente, nel corso dell'interazione tra i soggetti che provano ad attraversarli e quelli che devono controllarli. Ad esempio, i soggetti che provano ad attraversare i confini possono essere categorizzati come turisti o come migranti: i primi hanno maggiore libertà di movimento, i secondi molto meno. Ciò che Wonders però dimostra

---

62 F. Neresini, *Quando i numeri diventano grandi: che cosa possiamo imparare dalla scienza*, in *Rassegna Italiana di Sociologia*, 2015, 56(3-4), pp. 405-431. R. Brighi, *Il ruolo dei dati informatici nella costruzione della realtà. Tra vulnerabilità e esigenze di trasparenza*, Roma, Aracne, 2016.

63 B. Aragona, S. Stefanizzi, *Società digitale: interrogativi, aree di ricerca e ruolo della sociologia*, cit.

64 J.L. Austin, *How to Do Things with Words*, Cambridge (MA), Harvard University Press, 1975.

65 J. Butler, *Gender Trouble: Feminism and the Subversion of Identity*, New York-London, Routledge, 1990.

66 N.A. Wonders, *Global Flows, Semi-permeable Borders and New Channels of Inequality*, in L. Weber, S. Pickering (a cura di), *Borders, Mobility and Technologies of Control*, Dordrecht, Springer, 2006, pp. 63-86.

è che essere un "migrante" non è altro che l'esito di una categorizzazione[67], esito di una costruzione sociale. Essere categorizzati come migranti o come turisti dipende dall'esito della performatività del confine, che a sua volta dipende da genere, classe e "razza" delle persone che provano ad esercitare la propria libertà di movimento.

Dunque, come anche questi esempi illustrano, dire che i dati sono performativi significa affermare che essi siano in grado di costituire la realtà, di plasmarla. *I dati retroagiscono su chi li produce*. Un elemento di riflessione estremamente importante a questo punto è che la realtà viene ricostruita anche in base ai rapporti di potere comunque presenti nei processi di costruzione dei dati. Parlare della produzione di conoscenza in relazione alla tecnologia data-driven equivale a parlare delle strutture di potere insite nei processi di costruzione di dataset e software, nell'accesso ai dati e nella diversa possibilità che diversi soggetti hanno di comprendere come i dati vengono trasformati in informazioni.

Per produrre conoscenza tramite i big data ci si avvale di processi di *data mining*[68]. Il *data mining* è il processo con cui, partendo da grandi quantità di dati grezzi, si cercano schemi ricorrenti, relazioni e modelli nascosti che non sono immediatamente evidenti. Non si tratta solo di "leggere" i dati, ma di estrarre conoscenza utile da essi, spesso usando tecniche statistiche, algoritmi di machine learning e metodi matematici avanzati. Si tratta di un processo automatizzato, predittivo e induttivo. È automatizzato perché non è un'analisi manuale, ma un insieme di procedure algoritmiche che passano al setaccio milioni di dati. È predittivo perché non si limita a descrivere il passato, ma cerca di individuare tendenze future. È induttivo in quanto è volto alla ricerca di pattern emergenti, ovvero, parte dall'analisi dei dati senza che sia necessaria una teoria preesistente (si tratta, dunque, di *esplorazione* più che conferma di ipotesi. Si veda il paragrafo 3.3).

Il termine *data mining* indica l'insieme di tecniche computazionali volte a estrarre, da grandi insiemi di dati, schemi ricorrenti, relazioni e modelli nascosti che non sono immediatamente evidenti. Non si tratta di una semplice descrizione statistica, ma di un processo induttivo e predittivo che utilizza algoritmi e strumenti di machine learning per produrre nuova conoscenza a partire dai dati grezzi[69]. Volendo fare degli esempi, in ambito commerciale un processo di data mining su milioni di scontrini di supermercato può rivelare che chi compra birra

---

67 M. Tazzioli, *The Making of Migration: The Biopolitics of Mobility at Europe's Borders*, London, SAGE Publications, 2020.

68 D.J. Hand, H. Mannila, P. Smyth, *Principles of Data Mining*, Cambridge (MA), MIT Press, 2001.

69 D. Hand, H. Mannila, P. Smyth, *Principles of Data Mining*, Cambridge, MIT Press, 2001.

il venerdì sera tende anche a comprare patatine. Questo permette al negozio di fare offerte mirate o posizionare i prodotti vicini[70]. Nell'ambito della giustizia penale, il *data mining* può significare analizzare enormi database di arresti, denunce, movimenti GPS o persino post sui social media per cercare pattern nascosti e scoprire che in un certo quartiere, a una certa ora, avvengono più furti. Questo pattern può poi essere usato per decidere di aumentare la sorveglianza... con il rischio, però, di rafforzare i *bias* preesistenti (perché più pattuglie in quell'area porteranno a più arresti, che alimenteranno altri dati, creando un *feedback loop*).

Come dicevamo all'inizio del paragrafo, i dati non si limitano a descrivere la realtà, ma contribuiscono attivamente alla sua costruzione. Nel far ciò, riflettono e riproducono specifici rapporti di potere. Couldry e Mejías parlano a questo proposito di "colonialismo dei dati", per indicare un modello estrattivo che, pur in forme nuove, richiama le logiche del colonialismo storico. Se in passato venivano espropriate risorse materiali e forza lavoro, oggi ciò che viene estratto sono informazioni, comportamenti, relazioni sociali. I dati vengono raccolti, spesso senza un consenso consapevole, elaborati da algoritmi proprietari e utilizzati per orientare decisioni, pratiche di consumo o forme di sorveglianza. Un esempio emblematico è costituito dalle piattaforme digitali che, attraverso la raccolta continua di dati, determinano ciò che gli utenti vedono, le opzioni che hanno a disposizione e, in ultima istanza, le modalità con cui interagiscono con il mondo. In questo senso, i dati non solo rappresentano la realtà sociale, ma la plasmano in funzione degli interessi di chi controlla le infrastrutture tecnologiche. Questa dinamica implica una perdita di autonomia epistemica: la capacità delle persone e delle comunità di definire le proprie modalità di conoscenza viene subordinata a logiche esterne, spesso imposte da attori economici e tecnologici globali. Decolonizzare i dati, secondo gli autori, non significa semplicemente garantire una maggiore inclusione nei dataset, ma interrogare criticamente le fondamenta epistemologiche e politiche della produzione di conoscenza algoritmica[71].

Oltre a essere performativi, i dati digitali sono anche strumenti profondamente politici, in quanto incorporano e riflettono relazioni di potere che si manifestano nei processi di estrazione, gestione e utilizzo delle informazioni personali. Come osserva Sguazzini, la privacy è spesso ridotta a una questione tecnica o individuale, centrata sull'idea che i singoli utenti possano controllare consapevolmente il flusso dei propri dati. In realtà, le scelte che gli utenti com-

---

70 G. Ferguson, *The rise of big data policing*, cit.

71 N. Couldry, U.A. Mejias, *The decolonial turn in data and technology research: what is at stake and where is it heading?*, in *Information, Communication & Society*, 2023, 26(4), pp. 786-802.

piono – ad esempio accettare i termini di servizio o consentire l'uso dei cookie – avvengono all'interno di un'infrastruttura tecnologica opaca, in cui i reali margini di autonomia decisionale sono estremamente limitati. Ciò che conta, in questo contesto, non è solo la raccolta dei dati, ma il modo in cui essi vengono organizzati, interpretati e messi a valore da soggetti che detengono il controllo delle infrastrutture digitali. Questa dinamica evidenzia come la performatività dei dati non operi in uno spazio neutrale, bensì all'interno di un sistema di potere che definisce a monte cosa può essere conosciuto, da chi e a quali condizioni. Parlare di produzione di conoscenza attraverso i big data significa allora interrogare anche le logiche politiche che ne regolano l'uso, e riconoscere che la costruzione della realtà algoritmica avviene spesso senza un reale coinvolgimento dei soggetti da cui quei dati provengono[72].

Un esempio particolarmente efficace per comprendere la natura performativa dei dati è offerto dall'ambito della polizia predittiva. Kaufmann e Leese, analizzando il funzionamento di software algoritmici utilizzati nella sicurezza pubblica in Germania e Svizzera, introducono il concetto di *information in-formation* per descrivere la natura instabile, situata e trasformativa dei dati[73]. Con questa espressione, gli autori intendono sottolineare che i dati non sono entità fisse, già date e neutrali, ma sono continuamente *in formazione*, ossia soggette a processi di selezione, interpretazione, modifica e riutilizzo, sia da parte di attori umani (come poliziotti, analisti, operatori) sia da parte di sistemi automatici e infrastrutture digitali. I dati sono, in altre parole, "vivi" (*lively*), nel senso che mutano costantemente lungo tutto il loro ciclo di vita: dalla raccolta alla classificazione, dalla pulizia all'analisi, fino al loro riutilizzo in nuovi contesti. Questo carattere dinamico si manifesta, ad esempio, nel momento della registrazione iniziale di un evento criminale. La distinzione tra reati come furto, rapina o danneggiamento non è puramente oggettiva, ma dipende da come l'agente interpreta la scena, compila il modulo digitale e seleziona le categorie predefinite. Queste decisioni, spesso prese in condizioni di urgenza o sotto vincoli operativi, generano dati parziali e potenzialmente distorti. Tuttavia, tali dati alimentano i modelli di previsione, che a loro volta guidano le decisioni operative della polizia – ad esempio su dove concentrare le pattuglie. Questo genera un effetto circolare: le zone già sottoposte a sorveglianza producono più dati, che giustificano ulteriori interventi, in un ciclo autoreferenziale che tende a rafforzare disuguaglianze

---

72 M. Sguazzini, *Privacy politics: Power relations in the extraction, management, and use of personal data by non-state actors*, in *Rivista di Digital Politics*, 2022, II(3), pp. 399-422.

73 M. Kaufmann, M. Leese, *Information In-Formation: Algorithmic Policing and the Life of Data*, in V. Badalič, A. Završnik (a cura di), *Automating Crime Prevention, Surveillance, and Military Operations*, Cham, Springer, 2021, pp. 69-83.

preesistenti. La nozione di *information in-formation* aiuta dunque a comprendere come la performatività dei dati derivi non solo dai risultati finali prodotti dagli algoritmi, ma anche dai processi, spesso invisibili, attraverso cui i dati stessi prendono forma. In questa prospettiva, i dati non sono soltanto strumenti di conoscenza, ma anche dispositivi di potere che, attraverso pratiche quotidiane e tecnologie computazionali, contribuiscono attivamente alla costruzione della realtà sociale che pretendono di rappresentare.

Come osserva Ferguson, ciò che rende i big data davvero operativi non è soltanto la quantità o la varietà delle informazioni raccolte, ma l'insieme di tecnologie, algoritmi e potenza computazionale che permettono di renderli leggibili, comparabili e utilizzabili. «*What big data knows is one thing, but the technology used to manipulate and organize that data is the bigger thing*»[74]. Tuttavia, come sottolineano Kaufmann e Leese, questi strumenti operano su dati che non sono entità stabili e neutrali, ma prodotti dinamici di pratiche sociali, istituzionali e tecniche. La performatività dei dati, quindi, emerge dall'interazione tra la loro formazione situata e le infrastrutture computazionali che li classificano, li interpretano e li mobilitano. In questo senso, la costruzione della realtà algoritmica non è riconducibile né ai soli dati né ai soli algoritmi, ma va intesa come il risultato di un intreccio tra potere epistemico, pratiche operative e tecnologia. Come suggerisce la prospettiva decoloniale[75], sia i dati sia gli algoritmi si inscrivono in infrastrutture che riflettono gerarchie globali, interessi economici e rapporti di potere storicamente radicati. La produzione di conoscenza algoritmica non è dunque soltanto un processo tecnico, ma anche un progetto politico che contribuisce a definire chi può conoscere, cosa può essere conosciuto, e in quali termini.

---

74 G. Ferguson, *The rise of big data policing*, cit., p. 18.

75 N. Couldry, U.A. Mejias, *The decolonial turn in data and technology research*, cit.

4. Polizia e controllo data-driven

4.1 La nascita della polizia predittiva

Uno degli usi più rilevanti dei big data e delle tecnologie data-driven nel campo della giustizia penale si può rintracciare nello sviluppo della polizia predittiva. La polizia predittiva si avvale di big data e di algoritmi per valutare con quale percentuale di possibilità una persona possa commettere un reato o in che luogo è più probabile che un reato venga commesso. Infatti, la polizia predittiva può basarsi su informazioni centrate sulla persona (*person-based*) o sui luoghi (*place-based*). Nel primo caso, l'idea di fondo è che esista un piccolo gruppo di persone responsabile della maggior parte dei crimini violenti. Nel secondo caso, invece, è il classico assunto per cui il crimine avviene non in egual misura in tutti i posti ma è particolarmente concentrato solo in alcuni di essi. Questo tipo di polizia predittiva si rifà ad assunti criminologici ben strutturati circa la comprensione della criminalità, che hanno appreso che la criminalità non si distribuisce nello spazio in maniera uniforme, ma tende a concentrarsi in alcune zone. Sono assunti criminologici che utilizzano metodi quantitativi e che non si interrogano necessariamente sulle cause della criminalità quanto sull'intervento da mettere in campo nel territorio. Ovviamente, la polizia predittiva comporta tutta una serie di rischi legati ai big data che abbiamo anticipato nel capitolo precedente e che andremo ad approfondire in questo.

Prima però è utile chiarire un punto: la polizia ha da sempre fatto uso di dati e informazioni nella sua attività quotidiana: dai registri cartacei alle note di indagine, la raccolta di dati ha rappresentato un pilastro del lavoro investigativo e operativo. L'idea di prevedere e governare i comportamenti umani attraverso

strumenti di calcolo ha radici antiche. Già nel XVII secolo, in Europa, si sono diffuse pratiche come la raccolta di dati statistici e la formulazione di previsioni su fenomeni quali natalità, mortalità, rischio sociale e criminalità. Non si trattava soltanto di innovazioni tecniche. Come ha messo in luce Michel Foucault, questi strumenti costituivano delle vere e proprie *"tecnologie di potere"*. Secondo Foucault, le "tecnologie del potere" sono insiemi articolati di discorsi, istituzioni, norme giuridiche e pratiche sociali che compongono i dispositivi attraverso cui il potere agisce nella società in maniera pervasiva, capillare e normalizzante. Non si fondano sulla coercizione fisica, bensì su meccanismi come la sorveglianza – emblematicamente rappresentata dal Panopticon – e sulla produzione di saperi e di regole che orientano condotte e modi di percepire, influenzando così ogni aspetto della vita individuale e collettiva[1]. Le tecnologie di potere servono alla biopolitica[2] ovvero a quell'insieme delle pratiche di governo che mirano a conoscere, controllare e ottimizzare la vita collettiva, rendendo il potere indispensabile alla vita, un potere esercitato non più con la minaccia di "far morire e lasciar vivere", ma con la necessità di "far vivere o lasciar morire"[3]. Le nuove "tecnologie di potere" consentivano ai governi di trasformare masse di individui in una "popolazione" conoscibile, e quindi governabile. L'uso di metodi scientifici ha reso la società più "leggibile" e quindi più gestibile: la popolazione ha iniziato ad apparire come un insieme di regolarità prevedibili. In questo quadro, la polizia – intesa in senso ampio, non solo come corpo armato ma come insieme di pratiche e istituzioni dedicate all'ordine pubblico – ha acquisito un ruolo centrale[4]. Tuttavia, lo sviluppo delle tecnologie digitali e dei sistemi automatizzati ha trasformato radicalmente il modo in cui le informazioni vengono acquisite, elaborate e utilizzate. Non è cambiata tanto la natura dell'attività informativa, quanto piuttosto la sua scala, la sua profondità e la sua sistematicità[5]. L'integrazione di dati provenienti da fonti eterogenee – giudiziarie, commerciali, sociali – ha reso possibile un livello di sorveglianza e controllo che supera di gran lunga quello delle epoche precedenti, spostando il focus dei controlli di polizia da una

---

1 M. Foucault, *Sicurezza, territorio, popolazione. Corso al Collège de France (1977-1978)*, Milano, Feltrinelli, 2005.

2 M. Foucault, *Nascita della biopolitica. Corso al Collège de France (1978-1979)*, Milano, Feltrinelli, 2005.

3 M. Foucault, *La volontà di sapere*, Milano, Feltrinelli, 1978.

4 E. Gargiulo, *La Parola e la cosa*, in G. Fabini, E. Gargiulo, S. Tuzza, *Polizia: un vocabolario dell'ordine*, cit.; G. Campesi, *Genealogia della pubblica sicurezza: teoria e storia del moderno dispositivo poliziesco*, Verona, Ombre corte, 2009; M. Neocleous, *The Fabrication of Social Order: A Critical Theory of Police Power*, London, Pluto Press, 2000.

5 S. Brayne, *Predict and Surveil,* cit., p. 4.

logica reattiva a una logica predittiva e preventiva[6]. Questa trasformazione ha determinato una vera e propria evoluzione nei modelli di polizia.

Tuttavia, i cambiamenti di polizia non si devono solo all'avanzamento tecnologico ma anche al cambiamento culturale. Uno dei cambiamenti culturali più significativi è quello dell'anticipazione del rischio. La polizia ha sempre avuto come scopo prevenire la criminalità, facendo esperienza del passato per controllare quindi il presente ed evitare che si producano danni futuri:

> The modern police have always been inscribed with the potential to investigate past wrongs in order to prevent future harms to the social order. However, the future orientation of modern policing was historically limited to things like maintaining emergency preparedness for when things did go wrong and preventing crime and disorder from occurring by maintaining in the present a visible deterrent and the appearance of constant surveillance in public spaces[7].

Come osservano Dubber e Valverde, la polizia da sempre può essere considerata una sorta di "cerniera temporale": da un lato registra e gestisce ciò che è accaduto, dall'altro proietta l'azione di governo verso il futuro, cercando di prevenire i crimini prima che avvengano[8]. Adesso la questione è diversa. L'attività di polizia può essere proattiva, reattiva o retroattiva. Qualsiasi sia la sua inclinazione, per prevenire o reagire a qualcosa, servono comunque delle informazioni: tante, dettagliate, organizzate. Una considerevole parte del lavoro di polizia consiste da sempre nel raccogliere informazioni, solo che tale compito è stato amplificato esponenzialmente dall'utilizzo delle tecnologie.

Facendo riferimento al contesto statunitense, il primo modello è quello della polizia reattiva, dominante fino agli anni '60-'70, caratterizzata da interventi "post-evento" su chiamata o segnalazione. In questo paradigma, l'uso dei dati era limitato a registrazioni manuali e alla documentazione delle attività svolte[9]. Negli anni Ottanta, anche negli studi sulla polizia, era ormai chiaro che l'intervento reattivo della polizia non funzionasse contro la criminalità. Per questo si è iniziato a cercare di mettere in atto un sistema maggiormente proattivo rispetto alla criminalità. Dagli anni '80–'90 si afferma la polizia di prossimità

---

6 Ivi, p. 5.

7 B. Bowling, R. Reiner, J.W.E. Sheptycki, *The Politics of the Police* (5ª ed.), Oxford, Oxford University Press, 2019, pp. 31-32.

8 M.D. Dubber, M. Valverde, *Perspectives on the power and science of police*, in M. D. Dubber, M. Valverde (a cura di), *The New Police Science: The Police Power in Domestic and International Governance*, Stanford, Stanford University Press, 2006.

9 S. Brayne, *Predict and Surveil*, cit., pp. 3-4.

(*community policing*), che nasce come risposta alla crisi di legittimità delle forze dell'ordine e pone al centro la relazione tra agenti e comunità. In questo periodo, la raccolta di dati diventa più strutturata, supportata da strumenti statistici e geospaziali per identificare *hotspots* e pianificare le pattuglie[10]. Sono quindi emersi tutta una serie di modelli di polizia, ad esempio la *hotspot policing*, con l'idea di concentrare le forze di polizia in alcuni luoghi ed essere più efficaci contro la criminalità. Un punto di svolta fondamentale in questo processo è rappresentato dal programma CompStat, introdotto dal Dipartimento di Polizia di New York (NYPD) negli anni '90 sotto la guida di William Bratton. Questo sistema prevede la raccolta costante di dati su crimini, arresti e attività operative, utilizzati in incontri periodici (i *CompStat meetings*) per valutare le performance dei dirigenti e dei distretti. Il principio di "responsabilizzazione attraverso indicatori numerici" implica che ogni decisione operativa debba essere giustificata con dati misurabili, come il numero di arresti o la riduzione di specifici reati. Negli anni 2000 e soprattutto nel decennio successivo, si afferma infine il modello della polizia predittiva (*predictive policing*), che rappresenta una forma avanzata di *data-driven policing*. Questo approccio non si limita a monitorare i crimini già avvenuti, ma punta a prevedere reati futuri e a identificare individui o luoghi a rischio. «*In the contemporary period, data are used to predict or forecast future events and the automatation of police information systems makes possible systematic surveillance of far larger numbers of people with fewer personnel resources*»[11]. I dati utilizzati provengono non solo da fonti interne alla polizia (rapporti, schedature, archivi), ma anche da database commerciali, social media, sensori ambientali e piattaforme di sorveglianza urbana[12]. Questi vengono poi analizzati tramite "big data analytics"[13].

Oggi, dunque, si collezionano dati in maniera massiva. Ma sono dati grezzi, talmente tanti che a volte superano la capacità dell'istituzione di utilizzarli e rimangono sapere di polizia, o meglio: potenziale sapere di polizia, ma senza nessun sistema di accertamento della responsabilità giuridica davanti a un soggetto esterno[14].

Varie letture tendono a spiegare l'avvento della polizia predittiva come conseguenza dell'evoluzione tecnologica. Il lavoro di Brayne, invece, sposta l'attenzione da una spiegazione meramente tecnologica a un'analisi più strutturale.

---

10 Ivi, p. 9.

11 B. Bowling, R. Reiner, J.W.E. Sheptycki, *The Politics of the Police*, cit., p. 33.

12 S. Brayne, *Predict and Surveil*, cit., pp. 10-11, 14-16).

13 L. Bennett Moses, J. Chan, *Algorithmic prediction in policing: Assumptions, evaluation, and accountability*, in *Policing and Society*, 2018, 28(7), pp. 806-822.

14 B. Bowling, R. Reiner, J.W.E. Sheptycki, *The Politics of the Police*, cit., p. 33.

Invece di interpretare la polizia predittiva come semplice prodotto dell'innovazione algoritmica, Brayne mostra come essa nasca dall'intersezione di due processi più ampi: l'intensificazione della sorveglianza e l'ascesa dei big data[15].

In primo luogo, l'intensificazione delle pratiche di sorveglianza in generale si riferisce alla crescita quantitativa e qualitativa dei sistemi che raccolgono e classificano informazioni sulle persone nella vita quotidiana. Questo fenomeno si manifesta in due modi complementari: da un lato, attraverso un approfondimento (*deepening*) della sorveglianza su gruppi già considerati ad alto rischio – come persone in libertà vigilata, beneficiari di assistenza pubblica o comunità marginalizzate – che vengono monitorati con strumenti sempre più sofisticati e trasversali; dall'altro, attraverso un ampliamento (*widening*) delle popolazioni sotto osservazione, con pratiche di *dragnet surveillance* che raccolgono dati in maniera indiscriminata, anche su individui che non hanno mai avuto alcun contatto diretto con le forze dell'ordine. In questo modo, la sorveglianza diventa allo stesso tempo più profonda e più estesa: segue più da vicino chi è già oggetto di attenzione, ma al tempo stesso ingloba anche chi, in passato, ne sarebbe rimasto ai margini.

In secondo luogo, l'ascesa dei big data non si riferisce, secondo Brayne, solo a grandi quantità di informazioni, ma a un vero e proprio ambiente caratterizzato da quattro tratti distintivi: le tre V che in parte abbiamo già visto, ovverosia, vastità, velocità, varietà, a cui si aggiunge la digitalizzazione (la trascrizione e archiviazione elettronica di informazioni prima raccolte su supporti cartacei o in contesti limitati). Questa combinazione consente nuove forme di classificazione, collegamento e previsione: dati provenienti da ambiti diversi possono essere fusi in un'unica piattaforma, analizzati algoritmicamente e trasformati in mappe di rischio, punteggi individuali di pericolosità o sistemi di allerta automatica.

È nell'incontro tra questi due sviluppi – la sorveglianza che si fa più capillare e inclusiva e l'uso pervasivo dei big data – che, secondo Brayne, si radica la polizia predittiva. Infatti, l'incontro tra questi due sviluppi, che procedono autonomi e paralleli, ognuno con la propria genealogia, produce trasformazioni profonde: valutazioni discrezionali di rischio vengono sostituite o integrate da punteggi numerici, i dati vengono usati con finalità predittive piuttosto che solo reattive o esplicative, e database eterogenei vengono fusi in sistemi integrati che estendono la sorveglianza ben oltre l'ambito strettamente penale. In questa prospettiva, la polizia predittiva appare non tanto come il frutto inevitabile di nuove tecnologie, quanto come l'esito di una convergenza tra dinamiche di sorveglianza e potenzialità dei big data – è anche importante sottolineare che

[15] S. Brayne, *Big Data Surveillance: The Case of Policing*, cit.

esistono diversi software, non tutti utilizzano dati diffusi, tanti utilizzano solo dati di polizia.

Brayne collega l'intensificazione della sorveglianza all'evoluzione già avvenuta prima dell'avvento dei big data, richiamando concetti come *actuarial justice*[16] e la logica del rischio che aveva già investito la giustizia penale dagli anni '70-'80. In particolare, spiega che l'uso di strumenti di quantificazione e di modelli attuariali non nasce con i big data, ma già negli anni '20 vi erano tentativi di prevedere la recidiva e dagli anni '70-'80 le *sentencing guidelines* e le logiche attuariali hanno reso la valutazione del rischio un elemento strutturale di tribunali e correzioni. Negli anni '90, poi, si è assistito al passaggio da un modello di polizia reattivo (pattugliamenti casuali, risposta alle chiamate) a forme più proattive ed *evidence-based*, come l'*hotspot policing* e CompStat. Queste logiche già riflettevano una "giustizia del rischio" orientata all'anticipazione piuttosto che alla mera reazione. Inoltre, dopo l'11 settembre, *l'intelligence-led policing* ha ulteriormente consolidato la centralità della raccolta dati e dell'anticipazione del rischio nella sicurezza interna.

In questo senso, la *big data surveillance* di cui parla Brayne non è una rottura improvvisa, ma un'accelerazione di processi già in corso, riconoscibili nello sviluppo del diritto penale del nemico[17], la giustizia attuariale e il crescente interesse ad anticipare il rischio hanno predisposto il terreno sul quale i big data si sono innestati.

Secondo Brayne[18], l'introduzione dei big data nelle attività di polizia non va letta come una rottura totale rispetto al passato, ma piuttosto come un intreccio di continuità e discontinuità. Da un lato, molte pratiche tradizionali di sorveglianza vengono semplicemente amplificate e quantificate: le valutazioni discrezionali di rischio fatte dagli agenti, ad esempio, sono oggi trasformate in punteggi numerici; strategie come il pattugliamento delle aree "calde" (*hotspots*) sono riprese e rese più sistematiche grazie agli algoritmi; i registri cartacei sono sostituiti da database digitali, ma la logica sottostante resta simile. Dall'altro lato, l'uso dei big data introduce cambiamenti sostanziali: sistemi automatici di allerta permettono di monitorare un numero di persone mai visto prima; i database includono anche individui senza alcun contatto diretto con la polizia; soprattutto, i dati provenienti da istituzioni diverse (scuole, sanità, servizi sociali, settore privato) vengono integrati in piattaforme uniche, ampliando enormemente

---

16 M.M. Feeley, J. Simon, *The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications*, in *Criminology*, 1992, 30 (4), pp. 449-474.

17 S. Krasmann, *The enemy on the border: Critique of a programme in favour of a preventive state*, in *Punishment and Society*, 2007, 9(3), pp. 301-318.

18 S. Brayne, *Big Data Surveillance: The Case of Policing*, cit.

l'ambito della sorveglianza. In questa prospettiva, la polizia predittiva non è né una semplice prosecuzione delle tecniche del passato, né una cesura radicale: rappresenta piuttosto un punto di transizione in cui elementi già noti vengono riorganizzati e potenziati attraverso le infrastrutture digitali dei big data.

Altri autori forniscono altre spiegazioni circa la nascita della polizia predittiva.

Secondo Ferguson, l'ascesa della polizia predittiva e, più in generale, dei modelli di sorveglianza *data-driven* si fonda su due profondi cambiamenti culturali che hanno ridefinito il modo in cui le forze dell'ordine concepiscono e praticano il controllo sociale[19].

Il primo cambiamento riguarda l'evoluzione delle capacità tecniche e computazionali disponibili per l'analisi del crimine. Tecnologie come l'analisi predittiva, il *data mining*, l'analisi delle reti sociali e l'apprendimento automatico hanno reso possibile un salto qualitativo nella raccolta, archiviazione e interpretazione dei dati. La polizia, da sempre impegnata nella raccolta di informazioni su sospetti e reati, si trova ora in grado di accedere a database interconnessi, aggiornati in tempo reale e capaci di integrare fonti eterogenee: dati demografici, giudiziari, biometrici, ambientali e perfino informazioni ricavate da social media e fornitori privati. In questo nuovo ecosistema digitale, il sospetto non nasce più esclusivamente dall'osservazione diretta o dalla discrezionalità dell'agente, ma viene prodotto da algoritmi che classificano, calcolano e predicono il rischio individuale o territoriale. Ad esempio, la polizia può identificare un soggetto in strada attraverso il riconoscimento facciale, accedere al suo storico criminale, ricevere una valutazione algoritmica del suo livello di rischio e visualizzare immagini di sorveglianza delle sue attività nelle ore immediatamente precedenti. Questi strumenti promettono di «illuminare l'oscurità del sospetto»[20], ma al contempo, come già abbiamo visto sottolineato da Brayne, ampliano radicalmente l'ambito di chi può essere osservato, tracciato e controllato, rendendo potenzialmente ogni cittadino un oggetto di sorveglianza predittiva.

Il secondo cambiamento culturale è invece legato a una trasformazione nel rapporto tra polizia e comunità, in particolare quelle razzializzate. Il contesto è segnato da una crisi di fiducia profonda verso le forze dell'ordine, esplosa a seguito di una serie di omicidi di cittadini afroamericani disarmati – da Ferguson (Missouri) a Staten Island (New York), da Baltimore (Maryland) a Cleveland (Ohio) – che hanno portato alla nascita del movimento *Black Lives Matter* e a una mobilitazione nazionale contro la violenza e l'impunità della polizia. In ri-

[19] G. Ferguson, *The rise of big data policing*, cit.

[20] Ivi, p. 4.

sposta a questo clima di indignazione, le tecnologie predittive sono state presentate come strumenti di razionalizzazione dell'azione poliziesca, capaci di offrire una base apparentemente neutra, "oggettiva" e priva di pregiudizi razziali per la selezione dei target e delle aree da presidiare[21]. Tuttavia, la promessa di neutralità del *data-driven policing* appare, secondo Ferguson, più una narrazione strategica che una realtà verificabile:

> data-driven policing began to be sold as one answer to racially discriminatory policing, offering a seemingly race-neutral, "objective" justification for police targeting of poor communities. Despite the charge that police data remains tainted by systemic bias, police administrators can justify continued aggressive police practices using data-driven metrics. Predictive policing systems offer a way seemingly to turn the page on past abuses, while still legitimizing existing practices[22].

Ferguson sottolinea come i dati su cui si fondano questi sistemi siano spesso essi stessi il prodotto di pratiche storicamente discriminatorie. I database polizieschi riflettono e perpetuano decenni di attività mirate nelle comunità nere e latine, traducendo *bias* strutturali in metriche numeriche. Così, invece di eliminare la razzializzazione del controllo, la polizia predittiva rischia di legittimarla e istituzionalizzarla in forme più opache e meno contestabili, rafforzando una sorveglianza intensiva proprio sulle popolazioni già più colpite dalla repressione penale.

Anche secondo Ferguson esiste una continuità strutturale tra le pratiche tradizionali di polizia e le nuove forme di *big data policing*. In questa prospettiva, la *predictive policing* rappresenta un'evoluzione tecnologica di approcci preesistenti. Un esempio chiave è la *hotspot policing*, una strategia basata sulla mappatura delle aree ad alta incidenza criminale, che orientava le risorse in modo mirato nei luoghi statisticamente più a rischio di criminalità. Ferguson mostra come questa logica sia stata incorporata e potenziata dai sistemi predittivi, che non si limitano più a reagire a dati passati, ma cercano di anticipare i reati futuri, raffinando la selezione spazio-temporale degli interventi e incorporando nuove fonti di dati (es. social media, sensori urbani, reti di sorveglianza). Anche altre pratiche operative consolidate – come le *targeted patrols* e la *community policing* – sono state reinterpretate in chiave algoritmica, perdendo in parte la loro componente umana, relazionale e situata. Il passaggio non è solo tecnico, ma anche retorico:

---

21 *Ibidem*.

22 Ivi, pp. 5-6.

ciò che prima si basava sull'intuito o sull'esperienza viene ora presentato come "scientifico" e "oggettivo", grazie all'uso di algoritmi. Tuttavia, Ferguson mette in guardia dal rischio che questa apparente neutralità mascheri la riproduzione di *bias* preesistenti: i dati su cui si fondano questi sistemi sono spesso prodotti da pratiche poliziesche storicamente segnate da discriminazioni razziali. In questo senso, la *predictive policing* appare non come uno strumento nuovo e neutro, ma come un perfezionamento tecnologico di logiche operative già presenti, che rischia di amplificarne gli effetti distorsivi se non accompagnato da una riflessione critica sulle sue basi epistemologiche e sociopolitiche.

Delle basi epistemologiche e sociopolitiche della polizia predittiva si occupa un bel lavoro di recente pubblicazione, *Critical Perspectives on Predictive Policing. Anticipating proof?* a cura di Vasilis Galis, Helene O.I. Gundhus e Antonis Vradis. Secondo i curatori del volume, la polizia ha da sempre fatto affidamento sulla raccolta di informazioni per svolgere le proprie funzioni: documentare, indagare, classificare. Tuttavia, con l'avvento delle tecnologie digitali e dei sistemi algoritmici, questa attività informativa ha subito una trasformazione radicale. Non si tratta semplicemente di un aumento nella quantità dei dati raccolti, ma di un cambiamento profondo nella loro natura e nelle loro funzioni operative. La datificazione del lavoro di polizia implica un passaggio da un modello reattivo a un modello previsionale, in cui le informazioni raccolte non servono più solo a comprendere il passato o a documentare l'accaduto, ma a prevenire eventi futuri, anticipando reati non ancora commessi[23]. Questo nuovo paradigma si basa sull'estrazione e sull'elaborazione di segnali deboli e frammentari – come spostamenti, frequentazioni, comportamenti online – che vengono trasformati in prove anticipatorie (*anticipatory evidence*), capaci di giustificare l'intervento della polizia prima che si verifichi alcuna violazione effettiva[24].

In questo contesto, la funzione della polizia non è più semplicemente quella di reagire a una chiamata o indagare su un reato, ma di agire preventivamente sulla base di modelli predittivi, assumendo un ruolo quasi profetico nella gestione del rischio. Gli autori parlano di una vera e propria trasformazione epistemologica: la conoscenza poliziesca non si fonda più esclusivamente su fatti osservabili o testimonianze, ma su proiezioni statistiche e correlazioni probabilistiche che sostituiscono il concetto di prova con quello di previsione[25]. Secondo i tre autori, questo mutamento solleva interrogativi fondamentali sul piano normativo ed

[23] V. Galis, H. Oppen Gundhus, A. Vradis (a cura di), *Critical Perspectives on Predictive Policing: Anticipating Proof?*, Cheltenham-Northampton, Edward Elgar Publishing, 2025, pp. 6-7.

[24] Ivi, pp. 9-10.

[25] Ivi, p. 8.

etico, poiché sposta il baricentro della giustificazione dell'intervento poliziesco dalla colpevolezza alla potenziale pericolosità. In definitiva, la polizia predittiva ridefinisce non solo le pratiche operative, ma anche le categorie stesse attraverso cui il diritto, la sicurezza e la cittadinanza vengono articolati[26].

Un ulteriore spiegazione dell'emergere del big data policing guarda anche al ruolo dei singoli individui e in particolare di William Bratton.

Ferguson attribuisce un ruolo significativo a William Bratton nello sviluppo e nella diffusione della polizia predittiva, presentandolo come una figura centrale nella transizione verso un modello di sicurezza basato sull'analisi dei dati. Bratton, noto per il suo operato prima come capo della polizia a New York (NYPD) e poi a Los Angeles (LAPD), è descritto come un promotore strategico dell'uso di strumenti tecnologici per la gestione e la prevenzione del crimine. Ferguson sottolinea come Bratton abbia sostenuto l'evoluzione del sistema CompStat, inizialmente pensato come strumento di monitoraggio e accountability interna, verso un modello predittivo e proattivo. A Los Angeles, in particolare, sotto la sua guida, il LAPD ha collaborato con ricercatori e aziende per sviluppare programmi come PredPol, uno dei primi software di *predictive policing* implementati su larga scala. Ferguson evidenzia che Bratton ha anche svolto un ruolo importante come ambasciatore culturale e politico del *data-driven policing*, contribuendo a diffondere l'idea che l'analisi quantitativa e algoritmica potesse sostituire o perfezionare la discrezionalità tradizionale degli agenti. Il suo sostegno esplicito alla tecnologia ha contribuito a legittimare pubblicamente la narrazione secondo cui la polizia può diventare più efficiente, oggettiva e neutrale grazie all'uso dei dati. Bratton, quindi, come singolo, non è stato solo un innovatore operativo, ma anche un agente di cambiamento culturale, che ha contribuito a radicare nella pratica poliziesca contemporanea l'idea che la sicurezza urbana possa (e debba) essere governata attraverso modelli statistici e predittivi.

Anche secondo Karlsson e Galis[27], la vera consacrazione del termine *predictive policing* avviene negli Stati Uniti, soprattutto a partire dal 2008, quando William Bratton, allora capo del Los Angeles Police Department, e Sean Ma-

[26] In realtà, calata nel contesto italiano, questa affermazione non appare del tutto pacifica. Sembra infatti evidente che la polizia in Italia si occupa di pericolosità da sempre, non certo con l'avvento della tecnologia (si veda, a questo proposito, G. Campesi e G. Fabini, *Immigration Detention as Social Defence: Policing 'Dangerous Mobility' in Italy*, in *Theoretical Criminology*, 2020, 24, 1, pp. 50-70). Dunque, più che spostare il baricentro della polizia dalla colpevolezza alla pericolosità, si può affermare che la polizia predittiva rende evidente che la polizia si occupa di pericolosità più che di colpevolezza, mentre l'uso di tecnologie predittive anticipa ulteriormente la soglia di percezione e identificazione del pericolo.

[27] B. Karlsson, V. Galis, *POL-INTEL: Predictive policing and the politics of data integration in Denmark*, in V. Galis, H.O.I. Gundhus, A. Vradis (a cura di), *Critical Perspectives on Predictive Policing*, cit., pp. 84–103

linowski pubblicarono l'articolo *Police Performance Management in Practice: Taking COMPSTAT to the Next Level*. In quel testo, gli autori sostenevano che l'integrazione delle analisi di big data avrebbe permesso alla polizia di compiere un salto di qualità, passando da analisi "in quasi tempo reale" ad analisi "in tempo reale". L'idea era che un uso intensivo di modelli probabilistici potesse ridurre il numero di vittime, migliorare l'efficacia degli interventi e rafforzare la leadership di polizia. Questo entusiasmo tecnologico, che è stato definito *techno-solutionism*[28], ha progressivamente alimentato un immaginario secondo cui i dati e gli algoritmi sarebbero in grado di garantire una società più sicura, fino a ipotizzare, in chiave quasi utopica, un futuro "senza crimine". Parallelamente, però, si sono moltiplicate le critiche: diversi studiosi hanno evidenziato i rischi legati alla riproduzione di pratiche di polizia razzializzate e militarizzate, ai pregiudizi incorporati negli algoritmi e alle minacce per le libertà civili fondamentali.

Sebbene queste tecnologie siano spesso presentate come strumenti oggettivi e neutrali, Brayne sottolinea come esse amplifichino il potere discrezionale degli agenti, fornendo una nuova legittimità alle decisioni operative senza necessariamente renderle più giuste o trasparenti[29]. In questo senso, la tecnologia non elimina il giudizio umano, ma lo incanala e lo rafforza attraverso l'autorità dei numeri.

4.2 Polizia, potere discrezionale e tecnologia

Per discrezionalità di polizia si intende la libertà e l'autonomia di cui dispongono le e gli appartenenti alle forze dell'ordine nell'applicare la legge e nel prendere decisioni operative durante le attività di controllo e di indagine. La discrezionalità, insieme alla possibilità di fare uso della forza, è al cuore del potere di polizia[30].

La discrezionalità di polizia ha subito delle trasformazioni in seguito all'avvento delle tecnologie data-driven. Anzi, si può dire che le tecnologie data-driven si presentano come una risposta alla discrezionalità di polizia, che a volte rischia di scivolare nell'arbitrarietà. Tuttavia, a ben vedere, la tecnologia non im-

---

28 E. Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism*, New York, PublicAffairs, 2013.

29 S. Brayne, *Predict and Surveil*, cit.

30 E. Bittner, *The Functions of the Police in Modern Society: A Review of Background Factors, Current Practices, and Possible Role Models*, Washington (DC), National Institute of Mental Health, Center for Studies of Crime and Delinquency, 1970,

prime una trasformazione totale della polizia. Piuttosto, si possono rintracciare continuità e discontinuità con il passato. Proviamo ad approfondire.

La discrezionalità di polizia è oggetto di studio sin dagli esordi della sociologia della polizia[31]. Le ricerche empiriche su questa tematica, sin dagli albori della disciplina, mettono in luce che il diritto viene modellato dalle pratiche di polizia secondo le esigenze pratiche che le e gli agenti incontrano durante le attività di controllo[32]. La legge in azione (*law in books*) si differenzia da quella su carta (*law in books*). Con la polizia che funge da cinghia di trasmissione della legge scritta alla legge di fatto, può capitare che molte norme di legge vengano lasciate disapplicate, mentre altre vengano applicate in maniera ambigua, a seconda delle situazioni, dei contesti e delle persone[33].

Secondo Goldstein, la natura discrezionale del potere di polizia, ovvero la capacità delle e degli agenti di applicare la legge o astenersi dal farlo, è resa possibile dalla "bassa visibilità" entro cui operano. Infatti, gli agenti che operano su strada lo fanno da soli o in coppia, lontani dagli occhi della figura di supervisione, e possono decidere cosa riportare e cosa no: ciò che non viene riportato semplicemente rimane noto esclusivamente al controllore e al controllato[34]. Ovviamente, nel concetto di bassa visibilità è intrinseco un grave problema circa l'accountability e la responsabilità delle azioni delle forze di polizia: come si fa a rendere *accountable* un'istituzione se le azioni che compie sono invisibili?

È interessante riflettere su come la diffusione di immagini che caratterizza la società digitale, che provengano dalle videocamere di sorveglianza, dalle bodycam in dotazione agli agenti, ma anche dagli smart phone del pubblico, metta in dubbio la rilevanza del concetto di bassa visibilità oggi. Alcuni episodi di violenza della polizia sono saliti agli onori della cronaca proprio grazie alla diffusione delle immagini, ad esempio nel caso di George Floyd negli Stati Uniti, ma anche nel caso delle violenze all'interno del carcere di Santa Maria Capua Vetere dell'aprile 2020[35], ad esempio. Questo non significa che oggi la polizia non agisce in una situazione di bassa visibilità, non solo perché, accanto ad alcuni episodi di cui esistono le immagini, ci sono tanti altri episodi di abusi in cui le immagini non emergono, ma anche perché «la maggior parte degli incontri in

---

31 G. Fabini, *Il sapere sulla polizia*, in G. Fabini, E. Gargiulo, S. Tuzza, *Polizia: Un vocabolario dell'ordine*, cit.

32 E. Bittner, *The police on Skid-Row: A Study of Peace Keeping*, in *American Sociological Review*, 1967, 32(5), pp. 699-715.

33 G. Cordner, M. S. Scott, *Police Discretion and Its Control*, in G. Bruinsma, D. Weinsburd (a cura di), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, pp. 3587-3596.

34 J. Goldstein, *Police Discretion not to Invoke the Criminal Process: Low Visibility Decisions in the Administration of Justice*, in *Yale Law Journal*, 1960, 69, pp. 543-594.

35 L. Romano, *La settimana Santa. Potere e violenza nelle carceri italiane*, Napoli, Monitor, 2021.

strada avvengono con gruppi sociali relativamente deboli, con uno status debole nella politica della credibilità in una società gerarchica»[36]. Tuttavia, la bassa visibilità non riguarda solo la situazione straordinaria in cui si produce l'abuso di potere o addirittura l'uso illegittimo della forza, ma soprattutto l'attività ordinaria del lavoro di polizia e la scelta – frequente – di non applicare il diritto. La bassa visibilità di cui gode l'operato di polizia, per quanto il concetto possa essere innovato con le riflessioni sul ruolo della tecnologia in questo campo, è ancora un elemento valido nell'operato dell'istituzione.

Il punto è che l'esercizio della discrezionalità risulta, di fatto, pressoché inevitabile e probabilmente anche necessario. La necessità di decidere velocemente, unita all'imprevedibilità delle situazioni con cui le e gli agenti si confrontano, rende impossibile formulare regole ufficiali sufficienti a guidare ogni scenario. A causa dell'intrinseca vaghezza del diritto, la discrezionalità di polizia è al tempo stesso inevitabile e, con il tempo, tende a diventare pratica routinaria[37]. Questa anche per rispondere all'esigenza di rapidità: gli agenti devono prendere decisioni in modo rapido e continuativo e per questo è necessario avere orientamenti generali di tipo amministrativo piuttosto che direttive giuridiche rigide. La discrezionalità di polizia, dunque, si consolida spesso come prassi abituale, modellata da fattori estranei a considerazioni strettamente giuridiche—un tema che alimenta ampio dibattito nella letteratura.

Scrive Waddington che, «Se la polizia esercita il potere discrezionale in maniera routinaria, diventa essenziale per la ricerca identificare i criteri utilizzati dagli agenti nelle loro decisioni»[38]. Tali criteri possono essere giuridici, ma molto spesso risultano extra-giuridici: un certo tipo di cultura di polizia, l'orientamento politico, le campagne mediatiche del momento possono influenzare le scelte operative durante l'attività di controllo. Oggi, come vedremo meglio nei prossimi paragrafi, algoritmi e AI possono influenzare le scelte operative degli e delle agenti, in particolare nel determinare *dove* e verso *chi* dirigere la propria attenzione.

Già negli anni Settanta, la sociologia della polizia ha chiarito che nella logica di decisioni discrezionali rapide e routinarie, la prassi prevalente nella gestione di infrazioni minori è quella della disapplicazione della legge[39]. Di fronte a reati di lieve entità, gli agenti tendono a risolvere la situazione senza mobilitare gli strumenti del diritto. La tendenza della polizia a ignorare o a sottovalutare

---

36 B. Bowling, R. Reiner, J.W.E. Sheptycki, *The Politics of the Police*, cit., p. 232.

37 T. Newburn, R. Reiner, *Policing and the Police*, in M. Maguire, R. Morgan, R. Reiner (a cura di), *The Oxford Handbook of Criminology*, 5ª ed., Oxford, Oxford University Press, 2012, p. 809.

38 P.A.J. Waddington, *Policing Citizens. Authority and Rights*, London, UCL Press, 1999, p. 33.

39 L. Lustgarten, *The Governance of Police*, London, Sweet and Maxwell, 1986.

determinate violazioni è ampiamente riconosciuta tra i sociologi che studiano il fenomeno del *policing* dagli anni Sessanta ai primi anni Ottanta, molti dei quali adottano un approccio critico. Gli agenti, infatti, spesso «trascurano, ignorano, minimizzano o addirittura cancellano l'esistenza di numerose infrazioni legalmente perseguibili»[40]. Ciò dipende in parte dalla complessità del sistema normativo e in parte dalla riluttanza delle persone a denunciare certi reati. E in parte perché la situazione può essere risolta o governata anche senza ricorrere agli strumenti del diritto (con la minaccia del ricorso all'uso della forza, o con la minaccia di denunciare, con l'avvertimento, ecc.)

Paradossalmente, in un regime caratterizzato dalla disapplicazione, la scelta di far rispettare la legge anche per un'infrazione minore può costituire un significativo abuso di potere. Quando la discrezionalità si traduce in applicazione selettiva della legge, essa può generare seri abusi di potere con effetti discriminatori. L'applicazione selettiva della norma, infatti, può produrre forme di «discriminazione consapevole o inconsapevole basate sulle opinioni politiche, sull'aspetto personale, sullo status sociale o sulla razza»[41].

Un altro elemento già noto ai classici della sociologia sulla polizia è che l'attività di controllo è fortemente influenzata dalle pressioni legate alla produttività, misurata attraverso il numero di arresti o denunce. La costante pressione ad *apparire* efficienti mette il principio di efficienza in tensione con quello di legalità. Secondo Skolnick, gli agenti tendono spesso a privilegiare l'efficienza rispetto alla legalità, soprattutto in situazioni di emergenza. Infatti, per raggiungere un numero più elevato di arresti e rispondere alle pressioni dei superiori in questo senso, il controllo di polizia diventa più stringente verso alcuni gruppi sociali e in alcune zone rispetto ad altre[42].

La pressione alla produttività è un elemento che caratterizza la polizia anche nella società digitale.

Storicamente, la misurazione della produttività di polizia avveniva su base annuale; con COMPSTAT e sistemi analoghi si è passati prima a rilevazioni mensili, poi settimanali, fino ad arrivare a un monitoraggio quotidiano, talvolta aggiornato più volte al giorno. COMPSTAT è un software oggi adottato da centinaia di dipartimenti di polizia in tutto il mondo che combina la tecnologia di mappatura computerizzata con dati puntuali sulla criminalità, al fine di individuare i pattern della criminalità e indirizzare di conseguenza le risposte

40 P. K. Manning, *Police Work*, Cambridge (MA), The MIT Press, 1977, p. 199.

41 L. Lustgarten, *The Governance of Police*, cit., p. 15.

42 J. H. Skolnick, *Justice without Trial: Law Enforcement in Democratic Society*, New York-London-Sydney, John Wiley and Sons, 1966.

operative. I dipartimenti che ne fanno uso organizzano regolarmente riunioni di valutazione delle performance, durante le quali le e gli agenti e i loro superiori discutono dei dati più recenti relativi a criminalità e condotte operative. In tali occasioni, i superiori sono chiamati a rendere conto dei tassi di criminalità registrati nelle rispettive giurisdizioni[43]. Ma tali dati vengono utilizzati anche per tracciare e controllare l'attività operativa dei singoli (dove vanno, quanto tempo stazionano in un posto piuttosto che in un altro, ecc.). Dalle ricerche di Brayne sulla polizia di Los Angeles emerge che alcuni agenti preferiscono spegnere i dispositivi di tracciamento, proprio in protesta al fatto di essere controllati costantemente dai propri superiori.

I big data permettono un monitoraggio costante anche degli agenti, non solo da parte dei propri superiori ma, potenzialmente, da parte di tutta la comunità. Ferguson introduce l'idea di blue data, che si riferisce all'utilizzo dei big data non solo per orientare il lavoro di polizia ma anche per monitorare l'operato degli agenti. Se i sistemi di *big data policing* sono generalmente orientati alla raccolta e all'analisi di informazioni sui cittadini – in particolare su quelli appartenenti a comunità razzializzate e marginalizzate —, i *blue data* rappresentano per Ferguson la possibilità di rivolgere quello stesso sguardo analitico verso l'interno delle istituzioni di polizia. Rientrano in questa categoria dati come quelli provenienti dalle bodycam, i report sull'uso della forza, le statistiche sui fermi e sugli arresti, le mappe delle pattuglie e le metriche di performance degli agenti. In teoria, questo tipo di dati potrebbe essere impiegato per promuovere maggiore trasparenza, rilevare abusi sistemici, monitorare il rispetto delle procedure e, in ultima analisi, rendere la polizia responsabile del proprio operato[44].

Un ulteriore aspetto peculiare delle istituzioni di polizia è che il potere discrezionale tende ad aumentare man mano che si scende nella scala gerarchica[45]. Alla fine sono gli agenti di strada, i cosiddetti *rank-and-file officers*, a determinare l'esito concreto delle attività di polizia, poiché operano «laddove realmente conta: la strada»[46]. Nonostante occupino la base della catena di comando, gli *street-level bureaucrats*[47] esercitano un potere decisionale significativo, essendo che le politiche, ma anche le direttive dei superiori, nei fatti esistono solo se essi decidono di applicarle, altrimenti rimangono null'altro che lettera morta.

---

43 S. Brayne, *Predict and Surveil*, cit.

44 G. Ferguson, The rise of big data policing, cit.

45 J. Q. Wilson, *Varieties of Police Behaviour*, Cambridge (MA), Harvard University Press, 1968, p. 7.

46 R. Reiner, *The Politics of the Police*, Oxford, Oxford University Press, 2000, p. 86.

47 M. Lipsky, *Street-Level Bureaucracy: Dilemmas of the Individual in Public Service*, New York, Russell Sage Foundation, 1980.

Il dibattito sulla discrezionalità di polizia è ampio e sfaccettato. Alcuni sostengono che gli esiti dell'azione di polizia dipendono interamente dalle scelte dei singoli agenti, mentre altri che anche i dirigenti di polizia esercitano un potere discrezionale significativo, giacché decidono come allocare le risorse, quali strategie e strumenti adottare, a quali reati dare priorità e con quale grado di severità intervenire, in una situazione in cui la catena di comando ha un peso determinante. Sebbene meno visibili, queste decisioni risultano altrettanto cruciali nel determinare le forme di applicazione selettiva della legge[48]. Ai livelli più alti della gerarchia, la leadership della polizia stabilisce se un fenomeno debba o meno essere considerato un problema[49]. Un tema diventa oggetto di intervento soltanto quando i vertici decidono di riconoscerlo come tale. Queste scelte mettono in evidenza la natura intrinsecamente politica dell'attività di polizia[50], che comporta giudizi di valore, la tutela di alcuni interessi a scapito di altri e la gestione di rivendicazioni che concorrono tra loro per risorse scarse.

Anche qui è interessante interrogarsi sul ruolo della tecnologia data-driven, dal momento che le decisioni non dipendono più unicamente dai singoli poliziotti o dai loro superiori, ma anche dai software utilizzati nelle attività di prevenzione, controllo e indagine; quindi anche da chi sviluppa i software, spesso aziende private. Nello sviluppare un software, bisogna prendere molte decisioni circa quali minacce affrontare, quali indicatori considerare, quali teorie criminologiche impiegare. Oggi, quindi, la varietà di attori umani che partecipano al meccanismo decisionale durante le attività di controllo è aumentata. E, accanto ad essi, va considerato anche il ruolo degli attori non umani.

4.3 I rischi connessi ai controlli data-driven

Cosa è dunque la polizia predittiva? Ne esistono numerose definizioni. Noi qui proponiamo quella di Sarah Brayne, particolarmente calzante:

> Contrariamente all'analogia con *Minority Report* utilizzata in molti resoconti mediatici, l'attuale *predictive policing* non fa parte di un regime distopico di controllo in cui le persone vengono arrestate per crimini che non hanno ancora commesso. Al momento, almeno, è qualcosa di molto più banale. Con *predictive policing* si intendono semplicemente tecniche

[48] G. Fabini, E. Gargiulo, S. Tuzza, *Discrezionalità*, in G. Fabini, E. Gargiulo, S. Tuzza, *Polizia: un vocabolario dell'ordine*, cit., pp. 127-135.

[49] L. Lustgarten, *The Governance of Police*, cit.

[50] S. Tuzza, *Il dito e la luna*, Torino, Piemme Edizioni, 2021.

> analitiche utilizzate dalle forze dell'ordine per prevedere potenziali attività criminali. Si tratta di usare i dati per individuare gli attuali modelli di criminalità e orientare le risorse di pattugliamento, ad esempio stabilendo dove gli agenti dovrebbero recarsi e chi dovrebbero fermare. Queste tecniche si basano su un vasto corpus di ricerche che dimostrano come il crimine non sia distribuito in modo casuale tra persone o luoghi. Al contrario, sono i modelli legati alle condizioni ambientali dei luoghi, alle decisioni situazionali, ai recidivi e alle reti sociali a determinare quando e dove è più probabile che si verifichi un reato e chi abbia maggiori probabilità di esservi coinvolto. La tecnologia sfrutta questi schemi noti per supportare l'attività delle forze dell'ordine[51].

La convinzione che "i numeri non mentano" si è progressivamente radicata nelle pratiche delle forze dell'ordine. Da semplici supporti decisionali, la statistica e gli strumenti algoritmici sono diventati vere e proprie fonti di legittimazione delle scelte operative di polizia. Tale trasformazione ha prodotto un duplice effetto. In primo luogo, ha rafforzato la fiducia pubblica nell'illusione della neutralità algoritmica: si tende a credere che i numeri e i modelli matematici siano oggettivi e privi di *bias*. In secondo luogo, ha occultato i processi di costruzione dei dati, ovvero le modalità con cui le informazioni vengono raccolte, selezionate e interpretate, con tutti i loro limiti metodologici[52].

Ciò che pressoché tutti gli studi critici sulla polizia predittiva mettono in luce è che i sistemi di analisi predittiva – lungi dall'essere neutrali – si fondano su dataset costruiti nel tempo attraverso pratiche di polizia fortemente influenzate da criteri razziali, socioeconomici e spaziali. Lungi dal correggere questi *bias*, gli algoritmi tendono a riprodurli in forme meno visibili e quindi meno contestabili, conferendo una patina di scientificità a ciò che è, in realtà, una codificazione di pregiudizi sistemici.

Questa forma di *legittimazione algoritmica* delle decisioni di polizia è particolarmente problematica[53]. I numeri non sono più solo strumenti di analisi, ma diventano veri e propri dispositivi di autorità, capaci di ridurre lo spazio del dibattito democratico e giuridico[54]. A ciò si aggiunge l'uso di un linguaggio tecnico e l'opacità dei modelli computazionali – le cosiddette *black boxes* – che rendono difficile, se non impossibile, comprendere i meccanismi decisionali sottostanti. Questa opacità contribuisce a proteggere l'operato delle forze dell'or-

---

51 S. Brayne, *Predict and Surveil*, cit., p. 56.

52 G. Ferguson, *The rise of big data policing*, cit.

53 *Ibid*.

54 Si veda anche A. Završnik, *Algorithmic justice*, cit.; K. Hannah-Moffat, *Algorithmic risk governance*, cit.

dine dalla critica pubblica e dal controllo istituzionale. Inoltre, l'uso pervasivo di tali strumenti tende a ridurre la centralità del giudizio umano. In altre parole, gli agenti sono meno incentivati a valutare in modo autonomo le situazioni e ad assumersi la piena responsabilità delle proprie decisioni. Questo perché possono giustificare i loro interventi richiamandosi alle indicazioni dell'algoritmo, trasferendo di fatto la responsabilità a una tecnologia percepita come oggettiva e imparziale.

Vedremo tuttavia che, all'interno delle forze di polizia, esistono anche posizioni critiche rispetto all'uso di strumenti algoritmici e predittivi. Alcuni agenti segnalano infatti che tali strumenti finiscono per limitare le loro capacità di valutazione autonoma e di decisione, oltre a svalutare quello che viene definito *sapere di polizia*, cioè il sapere pratico derivato dall'esperienza diretta[55].

In ogni caso, pur esistendo pareri difformi circa l'efficacia, l'efficienza e l'opportunità di utilizzare strumenti predittivi anche tra gli addetti ai lavori, la *predictive policing* non solo riorienta le strategie operative, ma ristruttura profondamente le dinamiche di potere, accountability e agency all'interno del sistema di sicurezza. Stabilire l'*agency* – cioè individuare chi esercita un certo potere e in che modo questo produce effetti concreti – è fondamentale anche per poter attribuire la responsabilità delle azioni e delle conseguenze che ne derivano. Si tratta di una questione che abbiamo già visto emergere nelle riflessioni sul rapporto uomo-macchina nella società digitale. Tale questione non ha solo rilevanza teorica, ma implica conseguenze pratiche e di giustizia sociale[56]. Il rischio principale è che decisioni profondamente politiche – come la definizione di ciò che costituisce un "rischio" per l'ordine pubblico – vengano mascherate come valutazioni puramente tecniche, sottraendole così al controllo democratico e normativo[57].

Andiamo allora a vedere nello specifico quali sono questi rischi.

4.3.1 Discriminazione

Uno dei campi in cui il legame tra polizia e processi di razzializzazione è da sempre più evidente è la profilazione razziale durante l'attività di fermo e controllo, in inglese *stop and search*.

---

55 L. Neiva, R. Granja, H. Machado, *Big Data applied to criminal investigations: expectations of professionals of police cooperation in the European Union*, in *Policing and Society*, 2022, 32(10), pp. 1167-1179; L. Neiva, H. Machado, S. Silva, *The views about Big Data among professionals of police forces: A scoping review of empirical studies*, in *International Journal of Police Science and Management*, 2023, 25(2), pp. 208-220.

56 S. Milivojevic, *Crime and Punishment in the Future Internet*, cit., 2021.

57 G. Ferguson, *The rise of big data policing*, cit., pp. 20-33.

Svariate ricerche si sono concentrate nel mettere in luce la sovrarappresentazione delle minoranze razzializzate durante i fermi di polizia. In teoria, il potere di fermo e controllo è un potere investigativo, permesso solo quando vi sia un ragionevole sospetto che la persona che viene fermata stia commettendo qualche illecito. Il problema però è che le minoranze razzializzate vengono colpite più spesso[58].

Esiste una forte tradizione di studi su questo nel Regno Unito. Phillips e Bowling, per esempio, hanno dimostrato che gli asiatici hanno il doppio delle possibilità di essere fermati dalla polizia rispetto ai bianchi[59]; le persone nere sette volte. Ma il *racial profiling* è emerso anche in altri contesti: Toronto, New York, New Mexico, Parigi, Spagna, Finlandia, Svezia, Giappone[60], Italia[61]. I fermi di polizia producono e riproducono confini tra cittadini, creano gerarchie di appartenenza.

Il *racial profiling* non è visibile solo dai dati che dimostrano che le comunità razzializzate vengano fermate più spesso rispetto ai bianchi, ma anche da quei dati che mostrano che la percentuale di persone effettivamente denunciate dopo essere state fermate sia più altra tra i bianchi che tra le comunità razzializzate. Ovverosia, nel caso degli Stati Uniti, è più probabile che la polizia fermi per strada cittadini ispanici o afroamericani; ma una volta fermati, questi hanno più probabilità di essere rilasciati senza accuse a loro carico[62].

Inoltre, la ricerca ha iniziato a chiedersi quale sia effettivamente il vantaggio dell'utilizzo dello strumento di fermo: in fin dei conti, i benefici appaiono modesti e quantomeno esagerati nelle narrazioni, mentre i costi – sia sociali sia economici – sono sostanziali sebbene non riconosciuti[63].

Come più volte detto, si crede che i big data possano costituire uno strumento utile a limitare la profilazione razziale. Tuttavia, abbiamo visto che la tecnologia non è una soluzione, soprattutto per il fatto che, come dice Brayne, i dati sono sociali e si portano dietro le asimmetrie di potere delle società in cui essi si formano. Nel caso dell'utilizzo delle tecnologie data-driven, uno dei problemi

---

58 L. Weber, B. Bowling, *Stop and search in global context*, in *Policing and Society*, 2016, 21(4), pp. 353-356.

59 C. Phillips, B. Bowling, A. Parmar, *Ethnicities, racism, crime, and criminal justice*, in *The Oxford Handbook of Criminology*, Oxford, Oxford University Press, 2023.

60 B. Bowling, R. Reiner, J.W.E. Sheptycki, *The Politics of the Police*, cit., p. 137.

61 G. Fabini, *Polizia e migranti in città: Negoziare i confini nei contesti locali*, Roma, Carocci, 2023.

62 V.M. Weaver, A. Papachristos, M. Zanger-Tishler, *The Great Decoupling: The Disconnection between Criminal Offending and Experience of Arrest across Two Cohorts*, in *RSF: The Russell Sage Foundation Journal of the Social Sciences*, 2019, 5(1), 89-123.

63 C.R. Epp, S. Maynard-Moody, D.P. Haider-Markel, *Pulled Over: How Police Stops Define Race and Citizenship*, Chicago, University of Chicago Press, 2014.

sta proprio nei dati, ovvero, nella qualità del dato che viene utilizzato per predire il comportamento criminale: se il dato è già falsato dai processi di razzializzazione, questi non potranno che riprodurre tali processi di razzializzazione.

Come abbiamo detto, sistemi di polizia predittiva possono essere *place-based*, quindi basati sul luogo in cui si concentra la criminalità, o *person-based*, quindi atti a identificare i soggetti più inclinati a compiere reati. In entrambi i casi si agirà in un'ottica di prevenzione del crimine.

Un esempio di strumento di polizia predittiva basata sulla persona è l'Operazione LASER.

Operation LASER (*Los Angeles Strategic Extraction and Restoration*) è un programma di polizia predittiva avviato dal Los Angeles Police Department (LAPD) nel 2011. L'iniziativa combinava due approcci: da un lato l'uso di mappe termiche sui reati con armi da fuoco, dall'altro la redazione quotidiana di bollettini sugli *offenders* cronici.

La componente spaziale riprendeva le logiche del *hotspots policing*: i dati venivano aggregati per individuare i "corridoi caldi" della criminalità armata, e gli agenti erano incoraggiati a trascorrere più tempo in quelle aree, registrando le ore di pattugliamento nei rapporti giornalieri.

Parallelamente, l'unità di intelligence produceva i cosiddetti *Chronic Offender Bulletins*, liste di individui considerati a più alto rischio di reato. Questi bollettini includevano informazioni dettagliate (dati anagrafici, precedenti penali, affiliazioni, caratteristiche fisiche, veicoli, contatti con la polizia) e venivano distribuiti agli agenti, che erano invitati a interagire con queste persone durante i turni, non necessariamente per arrestarle, ma per raccogliere ulteriori dati.

Con il tempo, il sistema si è evoluto in un vero e proprio *punteggio di rischio*: i punti venivano attribuiti in base a vari criteri (ad esempio, crimini violenti, appartenenza a gang, precedenti con armi da fuoco, stato di libertà vigilata), oltre a un punto aggiuntivo per ogni "contatto di qualità" con la polizia. Poiché non esisteva una definizione univoca di "qualità", nella pratica qualsiasi fermo o compilazione di *Field Interview Cards*[64] contribuiva ad aumentare il punteggio. Queste schede venivano poi inserite nel sistema Palantir[65], una piattaforma

[64] Le *Field Interview Cards* (FI cards) sono schede cartacee a doppia faccia compilate manualmente dagli agenti in occasione di controlli sul campo. Contengono informazioni personali e identificative del soggetto fermato (nome, indirizzo, caratteristiche fisiche, affiliazioni, veicoli, precedenti) e uno spazio narrativo per annotazioni aggiuntive. Una volta digitalizzate e inserite nei database, costituiscono la base informativa per sistemi predittivi come Palantir, alimentando reti di collegamenti e profili di rischio.

[65] Palantir nacque come progetto per la sicurezza nazionale e ricevette i primi finanziamenti dalla società di venture capital della CIA, In-Q-Tel. Oggi rappresenta una piattaforma di integrazione e analisi dei dati ampiamente utilizzata dalle forze dell'ordine in diversi Paesi. Il suo punto di forza consiste nella capacità di raccogliere e combinare dati strutturati e non strutturati provenienti da fonti eterogenee – come schede di

di analisi dei dati utilizzata dalle forze dell'ordine per incrociare e visualizzare grandi quantità di informazioni. Esse contenevano informazioni personali, caratteristiche fisiche, affiliazioni, veicoli ed erano corredate da note discorsive degli agenti. L'aspetto critico è che la qualità del dato dipende dall'attività quotidiana degli agenti: più una persona viene fermata, più alto diventa il suo punteggio, il che giustifica ulteriori controlli, in un vero e proprio *feedback loop*. In questo modo, pregiudizi e pratiche di profilazione razziale non spariscono, ma vengono riformulati in un linguaggio tecnico e apparentemente neutro. Il sistema a punti è presentato come uno strumento conforme alla legge, pensato anzi per evitare accuse di profilazione esplicita. Tuttavia, nei fatti, contribuisce a rafforzare le disuguaglianze sociali e spaziali: le aree a basso reddito e a prevalenza minoritaria diventano quelle maggiormente pattugliate, e quindi maggiormente esposte a essere incluse nelle liste dei "soggetti cronici". Ne derivava una sorveglianza intensiva che appare formalmente "solo matematica", ma che nella pratica riproduce – e talvolta amplifica – i *bias* già presenti nelle pratiche di polizia tradizionali.

Uno strumento di polizia predittiva basata sul luogo è invece PredPol.

PredPol è uno dei sistemi di *predictive policing* più noti e controversi. Sviluppato da ricercatori dell'UCLA e commercializzato dal 2012, si tratta di uno strumento *place-based*, che elabora dati storici sulla criminalità per produrre *predicted boxes,* piccole aree quadrate (circa 150 metri per lato) in cui è più probabile che, nelle successive 12 ore, avvenga un reato. Gli agenti ricevono queste mappe all'inizio del turno e vengono incoraggiati a trascorrere più tempo in queste aree.

Il funzionamento di PredPol si basa su un algoritmo proprietario che utilizza tre input principali: il tipo di reato, il luogo e il momento in cui esso si è verificato. Il modello è costruito sulla teoria del *near-repeat*, secondo cui, dopo che un crimine si è verificato in un'area, le zone circostanti presentano un rischio

identificazione sul campo (FI), filmati di sorveglianza, social media, lettori di targhe, registri delle utenze e banche dati pubbliche – e di renderli accessibili attraverso un'unica interfaccia ricercabile. Grazie a queste funzioni, gli operatori possono mappare le relazioni tra individui, veicoli, indirizzi e incidenti tramite analisi di rete, visualizzando connessioni che altrimenti resterebbero invisibili. Per esempio, un agente può inserire il nome di un sospettato e ottenere una rete di persone, luoghi ed eventi collegati, costruendo così un profilo dettagliato delle sue associazioni. Palantir offre anche sistemi di allerta in tempo reale che notificano l'utente quando individui o targhe ricercate compaiono in nuovi flussi di dati, favorendo interventi tempestivi e proattivi. Tuttavia, la piattaforma solleva questioni etiche rilevanti. Integra infatti informazioni che non riguardano necessariamente attività criminali e presenta il rischio di *function creep*: i dati raccolti per un fine specifico possono essere riutilizzati per obiettivi di sorveglianza più ampi. Inoltre, gli algoritmi proprietari funzionano come una "scatola nera": non chiariscono in che modo stabiliscono connessioni o valutano i rischi. Questa opacità riduce la trasparenza e rende più difficile attribuire responsabilità agli attori che utilizzano il sistema.

aumentato di reati simili. L'algoritmo si alimenta di dieci anni di dati, attribuendo maggior peso a quelli più recenti, e genera così le mappe di rischio. Questo approccio ha mostrato risultati discreti per reati legati alla proprietà (ad esempio furti), mentre si è dimostrato molto meno efficace nel prevenire reati violenti. Il problema più rilevante, tuttavia, riguarda i suoi effetti sociali. PredPol non è neutrale: se i dati su cui si addestra riflettono pattern storici di sorveglianza e di arresti sproporzionati nelle comunità razzializzate, l'algoritmo finisce per riprodurre e amplificare queste stesse disuguaglianze. Le aree a prevalenza afroamericana o latino-americana, già fortemente pattugliate, risultano più frequentemente contrassegnate come "zone a rischio", generando un *feedback loop*: maggiore presenza della polizia produce più controlli, più segnalazioni e quindi più dati "negativi" che confermano falsamente la pericolosità di quei quartieri. In questo modo, una tecnologia presentata come "scientifica" e "oggettiva" rischia di mascherare pratiche di profilazione razziale già esistenti, rendendole meno visibili ma più radicate. PredPol diventa quindi un esempio emblematico di come il *predictive policing* possa tradursi non in un superamento dei *bias* umani, bensì nella loro istituzionalizzazione attraverso strumenti algoritmici.

Saremmo quindi in presenza di *black data*. Il termine "black data", secondo Ferguson, indica quei dati raccolti nel contesto delle attività di polizia che risultano opachi, incontestabili e potenzialmente pericolosi dal punto di vista delle libertà civili. Si tratta di un gioco concettuale con l'idea di "black box" – cioè un sistema il cui funzionamento interno è invisibile e inaccessibile – ma anche con implicazioni razziali, poiché questi dati riguardano in modo sproporzionato individui e comunità razzializzate, in particolare nere e latine.

Ferguson osserva che questi dati non sono sempre associati a condotte criminali verificate: possono includere segnalazioni anonime, informazioni non verificate, liste di individui "a rischio", contatti sociali tracciati o semplicemente presenze frequenti in determinate aree. Sono spesso raccolti automaticamente attraverso strumenti come telecamere, software di riconoscimento facciale, tecnologie di sorveglianza predittiva e database condivisi, e possono entrare a far parte di sistemi analitici complessi senza che i soggetti interessati ne siano consapevoli né abbiano la possibilità di correggere eventuali errori.

Uno degli aspetti più problematici del *black data* è la sua natura opaca e resistente alla trasparenza: è difficile sapere quali dati siano stati raccolti, come vengano interpretati e con quali conseguenze operative. Inoltre, questi dati alimentano modelli algoritmici che possono generare previsioni di rischio, influenzare le decisioni di pattugliamento o contribuire alla costruzione di "liste di soggetti di interesse", senza alcun processo di verifica indipendente.

In sintesi, il *black data* rappresenta una forma di conoscenza nascosta, che si sottrae al controllo democratico e alla possibilità di rettifica. Per Ferguson, questo tipo di dati è particolarmente insidioso perché unisce sorveglianza invisibile, assenza di responsabilità e rafforzamento dei *bias* sistemici, creando un ambiente in cui la criminalizzazione preventiva può espandersi senza opposizione efficace.

4.3.2 Privacy

L'utilizzo dei big data da parte delle forze di polizia solleva questioni cruciali di privacy. Proviamo a vederli nello specifico di alcuni sistemi utilizzati, negli Stati Uniti e in Europa.

Palantir – che abbiamo incontrato nel sottoparagrafo precedente – non è un semplice archivio ma una piattaforma capace di integrare dataset diversi e renderli interrogabili in tempo reale. Gli operatori possono formulare domande specifiche o impostare allarmi, e ogni ricerca effettuata viene registrata dal sistema e si traduce a sua volta in un nuovo dato. In questo modo, anche il solo fatto che un soggetto venga ripetutamente interrogato nel sistema può alimentare sospetti, dando origine a catene di pregiudizio e stereotipi[66]. Il Progetto LASER, che come abbiamo visto è stato sviluppato e impiegato in contesto statunitense mira a identificare individui ad alto rischio di commettere o subire violenza armata, e combina diversi set di dati per costruire un "*criminal chronic offender bulletin*" utilizza dati che includono arresti precedenti, frequenza delle interazioni con la polizia, appartenenza nota o sospetta a gang, dati geografici relativi alla presenza in "zone ad alta criminalità", informazioni tratte da reti sociali e database interni (es. connessioni tra sospettati). Il progetto risulta opaco, mancano controlli di legalità e gli individui coinvolti non hanno la possibilità di contestare la propria classificazione. Il programma è stato attivo senza sufficiente controllo pubblico e senza la notifica diretta agli individui profilati, violando, secondo Ferguson, principi basilari di privacy e trasparenza negli Stati Uniti[67].

Gli Automatic License Plate Readers (ALPR) mettono invece in luce un ulteriore aspetto problematico che riguarda l'abbassamento progressivo delle soglie di inclusione nei database. Gli ALPR sono dispositivi montati su auto di pattuglia o collocati agli incroci stradali che fotografano sistematicamente targhe e veicoli, associando data, ora e coordinate geografiche. Si tratta di strumenti di sorveglianza di massa che raccolgono informazioni su chiunque, anche su individui non sospettati di alcun reato. Non è necessario un contatto diretto con

---

66 S. Brayne, *Predict and Surveil*, cit.

67 G. Ferguson, *The rise of big data policing*, cit., p. 104.

la polizia per esservi registrati. In alcuni contesti, come l'installazione di ALPR presso i pronto soccorso, questa pratica ha persino scoraggiato persone a rivolgersi alle strutture sanitarie per timore di essere registrate[68]. Inoltre, attraverso l'analisi retrospettiva di questi dati, la polizia può ricostruire gli spostamenti passati di un individuo, violando il diritto a muoversi anonimamente nello spazio pubblico[69]. Inoltre, ALPR usa dati originariamente prodotti per scopi civili – ad esempio pagamenti elettronici o registrazioni commerciali – che vengono successivamente piegati a finalità di *law enforcement*. A ciò si aggiunge l'incertezza sulla durata della conservazione dei dati e l'assenza di regole uniformi che stabiliscano limiti chiari all'uso delle informazioni raccolte[70].

Ferguson discute anche il progetto chiamato Collaborative Assessment and Management of Suicidality (CAMS), in cui si condividono dati tra scuole, servizi di salute mentale e polizia per identificare giovani potenzialmente violenti. I dati raccolti possono includere presenze scolastiche, comportamenti disciplinari, valutazioni psicologiche, segnalazioni di disagio mentale, dati sanitari e storici di interventi sociali. Queste collaborazioni creano un ecosistema di sorveglianza istituzionale che mette a rischio la privacy dei soggetti più vulnerabili, senza garanzie sufficienti sul consenso, sull'uso corretto delle informazioni o sulla possibilità di rettifica[71].

I rischi per la privacy legati alla polizia predittiva derivano principalmente dalla perdita di anonimato nello spazio pubblico e dalla costante raccolta di dati comportamentali, anche su cittadini che non sono sospettati di alcun reato. Questo significa che dati su individui innocenti vengono raccolti, analizzati e utilizzati per anticipare comportamenti futuri, spesso senza che questi soggetti ne siano consapevoli o abbiano fornito alcun consenso (p. 97-98). Il monitoraggio tramite telecamere intelligenti e software di riconoscimento facciale, possono identificare ogni movimento o interazione urbana, anche in assenza di un sospetto specifico (p. 100-101). Le forze dell'ordine possono utilizzare dati raccolti da fonti come social media, registri commerciali, scuole e sistemi sanitari, creando una visione completa ma invasiva della vita privata di un individuo. Inoltre, spesso le persone monitorate non sanno di essere profilate, non possono accedere ai dati raccolti su di loro e non hanno modo di contestare l'inclusione in una zona ad alto rischio o in una "lista di sorvegliati"[72].

---

68 S. Brayne, *Predict and Surveil*, cit.
69 G. Ferguson, *The rise of big data policing*, cit., pp. 101-102.
70 S. Brayne, *Predict and Surveil*, cit.
71 G. Ferguson, *The rise of big data policing*, cit., p. 107.
72 Ivi, pp. 97-106.

Il riconoscimento facciale in tempo reale (Live Facial Recognition, LFR) rappresenta una delle forme più invasive di sorveglianza contemporanea, con implicazioni profonde per la privacy e per i diritti fondamentali. Come sottolineano Papada e Vradis, l'uso diffuso di queste tecnologie nello spazio urbano produce un regime di sorveglianza di massa, in cui la semplice presenza nello spazio pubblico può trasformarsi in un atto sospetto, potenzialmente oggetto di schedatura e analisi biometrica[73]. Il volto, parte intima e identitaria del corpo, diventa un dato costantemente catturato, archiviato e confrontato con database di polizia, riducendo l'anonimato urbano e trasformando la città da luogo di libertà a spazio di sospetto permanente. A questi rischi diretti si sommano le dinamiche di sorveglianza interiorizzata: i cittadini, consapevoli della possibilità di essere monitorati in ogni momento, tendono a modificare i propri comportamenti quotidiani, limitando spostamenti, evitando determinate interazioni o rinunciando alla partecipazione a eventi pubblici. Tale processo, che richiama da vicino la logica foucaultiana della disciplina e del *panopticon*, conduce a una forma di autocontrollo diffuso e alla progressiva normalizzazione della sorveglianza. È emblematico il caso della South Wales Police a Cardiff, che aveva introdotto sistemi di LFR per monitorare eventi pubblici e strade cittadine, confrontando i volti dei passanti con liste di persone di interesse. Nel 2020 la Court of Appeal per Inghilterra e Galles – quindi in un contesto significativamente diverso da quello degli Stati Uniti – ha dichiarato tale pratica illegale, ritenendo che violasse il diritto alla privacy sancito dalla Convenzione europea dei diritti dell'uomo, le normative sulla protezione dei dati e i principi di uguaglianza. La sentenza ha messo in luce gravi carenze: criteri opachi per l'inclusione nelle *watchlists*, assenza di linee guida chiare per limitare la discrezionalità della polizia, mancata valutazione d'impatto sui diritti fondamentali. Tuttavia, questa decisione non ha comportato l'abbandono definitivo delle tecnologie di riconoscimento facciale. Al contrario, esse tendono a riemergere in forme ridefinite e circoscritte, ad esempio per il monitoraggio di grandi eventi sportivi, concerti o aree commerciali, spesso giustificate da esigenze di sicurezza. Tale persistenza dimostra come, anche di fronte a limiti giuridici espliciti, la pressione istituzionale e tecnologica favorisca la continuità della sorveglianza biometrica, aggravando i rischi di erosione della privacy, discriminazione algoritmica e compressione delle libertà civili nello spazio urbano[74].

---

[73] E. Papada, A. Vradis, *The birth of spatial transgression: genealogies and regulatory instruments in the use of facial recognition technologies in the UK*, in V. Galis, H.O.I. Gundhus, A. Vradis (a cura di), *Critical Perspectives on Predictive Policing: Anticipating Proof?*, Cheltenham-Northampton, Edward Elgar Publishing, 2025, pp. 43-64.

[74] *Ibid.*

4.3.3 L'ingerenza del privato

Abbiamo già visto che la polizia da sempre ha utilizzato i dati nelle proprie attività di prevenzione, indagine e controllo e che se prima questi erano conservati in forma cartacea, adesso lo sono in digitale. Uno dei più grossi cambiamenti però è l'intervento del settore privato in questo campo.

Esiste un settore privato in espansione che si occupa di collezionare e vendere i dati personali dei cittadini. Molte agenzie integrano i propri database interni con informazioni commerciali, come registri dei social media, dati sul traffico o comportamenti dei consumatori, acquistati da imprese private. Questa pratica consente analisi più ampie, ma solleva preoccupazioni sull'accuratezza dei dati, sul loro uso etico e, non da ultimo, sulle implicazioni per la privacy derivanti dall'integrazione di tali dati. Le aziende private forniscono anche dati direttamente alle forze dell'ordine[75].

Il ruolo delle agenzie private nel collezionare e nell'utilizzo dei dati è di primaria importanza per vari motivi. Ad esempio, tramite l'intervento di compagnie private dedicate alla vendita di dati personali, possono arrivare all'attenzione delle forze dell'ordine anche i dati di persone che di solito non facevano esperienza di controlli di polizia. Oltretutto, la tipologia di dati a cui la polizia arriva è del più svariato tipo, tracciate nei più svariati modi. Dunque, anche dati che non sono direttamente interessanti per scopi di *law enforcement* o condotte non penalmente rilevanti possono entrare nella sfera d'azione della polizia.

Facciamo un esempio. Glouftsios e Leese mostrano come i dati PNR (Passenger Name Record) – inizialmente raccolti dalle compagnie aeree per scopi commerciali – siano diventati una pietra angolare delle operazioni di sicurezza pubblica. Le compagnie aeree, in quanto entità private, raccolgono e trasmettono i dati PNR alle Passenger Information Units (PIU) gestite dai governi, in base a quadri normativi come la Direttiva PNR dell'Unione Europea. Questi database contengono informazioni sensibili sui passeggeri, come identità, itinerari di viaggio, metodi di pagamento e preferenze. Sebbene la raccolta sia pensata per la gestione dei clienti, il loro riutilizzo a fini di sicurezza statale rivela la privatizzazione di fonti di dati essenziali. Agendo come intermediari, le compagnie aeree trasformano dati commerciali in intelligence operativa, incorporando processi privati nell'ecosistema più ampio della sorveglianza. La dipendenza da attori privati va oltre la raccolta dati, includendo anche le infrastrutture tecnologiche che permettono l'elaborazione e l'analisi dei big data. Le PIU si affidano a strumenti di integrazione e software, spesso sviluppati o gestiti in collaborazione

[75] S. Brayne, *Predict and Surveil*, cit.

con fornitori privati, per analizzare e incrociare i dati PNR con altri database di sicurezza pubblica, come le liste di sorveglianza o i sistemi di immigrazione. Questi strumenti permettono ai governi di operare su dataset enormi, ma al contempo inseriscono interessi privati nei quadri di sicurezza pubblica. Inoltre, le imprecisioni intrinseche dei dati PNR autocompilati – come errori di battitura o informazioni incomplete – richiedono ulteriori misure di controllo della qualità. Le compagnie aeree, in quanto fornitori di dati, influenzano significativamente la qualità e l'affidabilità delle informazioni trasmesse alle PIU, modellando indirettamente l'efficacia delle analisi di sicurezza[76].

Non è solo sulla raccolta di dati che il settore privato agisce. Il settore privato svolge un ruolo fondamentale anche nel plasmare il modo in cui le forze dell'ordine utilizzano i big data per il controllo, la prevenzione e l'indagine dei reati. I dipartimenti di polizia si affidano sempre più frequentemente (ancora poco in Italia, fortunatamente) a software di polizia predittiva sviluppati da aziende private, integrando nei loro sistemi algoritmi proprietari.

Proprio il fatto che alcuni algoritmi sono di proprietà di compagnie private alimenta l'opacità di questi strumenti. Come abbiamo visto, molti software funzionano come "scatole nere", i cui meccanismi interni restano inaccessibili sia agli agenti di polizia sia al pubblico. Questo avviene non solo a causa delle lacune in materie come *computer science* o informatica, fondamentali per comprendere il funzionamento degli algoritmi, ma anche a causa di vincoli legati alla proprietà intellettuale.

Abbiamo visto quali possono essere le conseguenze della mancanza di trasparenza: la difficoltà a stabilire chi ha la responsabilità per le decisioni che vengono prese (l'uomo o la macchina?) e il fatto che per le forze di polizia stesse diventa difficile sapere come la macchina è arrivata al risultato finale della sua analisi e, quindi, valutare l'accuratezza di tale esito. Per ovviare a questo problema, alcuni dipartimenti di polizia hanno scelto di sviluppare software alternativi interni (in Italia è il caso del software Xlaw nella questura di Napoli), con l'obiettivo di ridurre la dipendenza dai privati e garantire una maggiore comprensione dei processi algoritmici.

Il rapporto tra le forze dell'ordine pubbliche e le imprese tecnologiche private influenza non solo lo sviluppo degli strumenti di analisi criminale, ma anche il modo in cui le teorie criminologiche vengono applicate.

Lo sviluppo e l'applicazione di algoritmi per l'analisi criminale illustrano la profonda interconnessione tra agenzie pubbliche di polizia e imprese tecnologi-

---

[76] G. Glouftsios, M. Leese, *Epistemic fusion: Passenger Information Units and the making of international security*, in *Review of International Studies*, 2023, 49(1), pp. 125-142.

che private, a tal punto che partnership pubblico-private finiscono per guidare l'evoluzione della polizia algoritmica, fondendo teorie criminologiche con le potenzialità dei sistemi di big data.

Nel suo studio sul Los Angeles Police Department (LAPD), Brayne documenta come aziende private come Palantir e PredPol sviluppino e forniscano tecnologie predittive adottate dalle forze dell'ordine per potenziarne le capacità analitiche. Come abbiamo visto, Palantir è originariamente finanziata dal fondo di venture capital della CIA e integra vasti dataset – dai registri criminali e i rapporti sul campo fino all'attività sui social media e ai dati dei servizi pubblici – consentendo alla polizia di creare reti dettagliate di relazioni e di identificare schemi di comportamento criminale. PredPol, invece, utilizza dati storici sulla criminalità e concetti criminologici come la *Near-Repeat Hypothesis* per prevedere dove è più probabile che avvengano reati, indirizzando le pattuglie verso aree ad alto rischio. Questi strumenti si basano su fondamenti teorici come la *Rational Choice Theory*, che presuppone che i criminali agiscano in maniera prevedibile in base a fattori ambientali e situazionali. Trasformando tali teorie in modelli algoritmici, le imprese private influenzano non solo il modo in cui la criminologia viene applicata, ma anche come queste teorie vengono interpretate e quali acquisiscono maggiore importanza e impatto nella pratica.

Le aziende private commercializzino i loro strumenti come soluzioni efficienti e accurate nella loro capacità predittiva. Queste tecnologie presentano i propri algoritmi come neutrali e guidati dai dati, sostenendo di ridurre i *bias* sostituendo il giudizio umano con metriche quantificabili. Tuttavia, tali strumenti sono oggettivi solo quanto i dati e le ipotesi su cui si basano. Molti algoritmi si fondano su definizioni ristrette di criminalità, escludendo fattori strutturali come povertà o disuguaglianza, che invece molte teorie criminologiche – forse quelle più critiche – considerano fondamentali per comprendere i fenomeni criminali[77].

La collaborazione tra attori pubblici e privati incide anche sulla diffusione del sapere criminologico. Se da un lato le teorie criminologiche guidano la progettazione dei modelli predittivi, dall'altro la commercializzazione di tali strumenti ne restringe spesso l'applicazione a risultati misurabili e vendibili. Concetti come l'*hotspot policing* o i punteggi di valutazione del rischio dominano i framework algoritmici, mentre teorie sociali più ampie che affrontano le disuguaglianze sistemiche o le cause profonde della criminalità vengono marginalizzate. Questa dinamica riflette la tensione tra le radici accademiche della criminologia e la sua

[77] M. Kaufmann, S. Egbert, M. Leese, *Predictive policing and the politics of patterns*, in *British Journal of Criminology*, 2019, 59(3), pp. 674-692.

traduzione operativa in strumenti algoritmici progettati per mercati guidati dal profitto.

Questo certamente si deve anche a un cambiamento del sapere criminologico, che per adeguarsi alle nuove richieste, ha rinnovato le proprie spiegazioni teoriche, dando sempre più spazio, ad esempio, alle metodologie quantitative piuttosto che le qualitative. Come spiegano efficacemente Karlsoom e Galis, queste trasformazioni della criminologia hanno rappresentato il motore per la costruzione di modelli quantitativi che, in epoca contemporanea, sono stati progressivamente digitalizzati e automatizzati[78]. Un esempio significativo è offerto da Van Brakel, che ricorda come la diffusione delle teorie di prevenzione situazionale negli anni Novanta abbia favorito lo sviluppo dell'analisi dei *crime hot spots* e, successivamente, la creazione nel Regno Unito di una delle prime applicazioni di polizia predittiva, nota come *ProMap*[79].

Se le collaborazioni con il settore privato potenziano le capacità analitiche della polizia, comportano anche il rischio non solo di perpetuare *bias* e restringere l'orizzonte dell'indagine criminologica, ma anche di privilegiare gli interessi commerciali rispetto alla responsabilità pubblica. Infatti, i software proprietari tendono a privilegiare logiche di profitto e di mercato rispetto alla trasparenza e alle considerazioni etiche legate al loro uso.

Le aziende private giocano anche un ruolo significativo nel determinare come questi strumenti vengano adottati e utilizzati. Imprese come Palantir promuovono attivamente i propri prodotti attraverso conferenze per le forze dell'ordine, presentando casi d'uso che sfumano i confini tra applicazioni militari e sicurezza pubblica[80]. Gli interessi del settore privato influenzano così lo sviluppo degli algoritmi di analisi criminale, privilegiando sistemi proprietari rispetto a soluzioni trasparenti e collaborative[81]. Con l'evoluzione delle tecnologie di polizia predittiva, la dipendenza dai fornitori privati rischia di consolidare pregiudizi non controllati nelle pratiche delle forze dell'ordine, sottolineando la necessità di una maggiore supervisione anche da parte di organismi esterni e dell'opinione pubblica e di un'analisi critica di tali partnership[82]. Questa mancanza di trasparenza rende difficile per le

---

78 B. Karlsson, V. Galis, *POL-INTEL: Predictive policing and the politics of data integration in Denmark*, cit., pp. 123 ss.; S. Egbert, M. Leese, *Criminal Futures: Predictive Policing and Everyday Police Work*, London-New York, Routledge, 2021.

79 R.V. Brakel, *Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing*, in B. van der Sloot, D. Broeders, E. Schrijvers (a cura di), *Exploring the Boundaries of Big Data*, Amsterdam, Amsterdam University Press, 2016.

80 S. Brayne, *Predict and Surveil*, cit.

81 K. Hannah-Moffat, *Algorithmic risk governance*, cit.

82 M. Kaufmann, S. Egbert, M. Leese, *Predictive policing and the politics of patterns*, cit.

forze dell'ordine – e per il pubblico – valutare il funzionamento di tali algoritmi o mettere in discussione le assunzioni su cui si fondano.

4.3.4 Conseguenze sociali

Un aspetto centrale del controllo data-driven riguarda le conseguenze sociali dell'uso dei big data da parte della polizia. In linea teorica, la digitalizzazione potrebbe avere un effetto positivo, perché rende le decisioni più trasparenti e riduce la dipendenza esclusiva dal giudizio discrezionale degli agenti. Ad esempio, un algoritmo potrebbe correggere alcuni pregiudizi impliciti che storicamente hanno segnato le pratiche di polizia, come l'associazione automatica tra criminalità e appartenenza etnica. Inoltre, i dati digitali consentono di "sorvegliare i sorveglianti": cioè di monitorare come la polizia utilizza le informazioni, rendendo così più controllabili le sue attività. Tuttavia, nella pratica i big data tendano spesso a rafforzare e riprodurre disuguaglianze sociali preesistenti. Questo avviene in tre modi principali. In primo luogo, la sorveglianza diventa più profonda per chi è già nel raggio d'azione della giustizia penale: le persone con precedenti, o già classificate come "a rischio", vengono seguite attraverso una molteplicità di banche dati che si intrecciano, moltiplicando le occasioni di controllo. In secondo luogo, si assiste a un ampliamento della sorveglianza verso nuove popolazioni: i sistemi digitali includono dati di individui che non hanno mai avuto un contatto diretto con la polizia, creando un'enorme "rete a strascico" che ingloba fasce sempre più ampie di cittadini. Infine, questa nuova configurazione può produrre effetti collaterali paradossali: per timore che le informazioni personali possano finire nei database della polizia, alcuni cittadini evitano scuole, ospedali o servizi sociali, cioè proprio quelle istituzioni fondamentali per l'integrazione e il benessere collettivo[83].

Se da un lato i big data aprono la possibilità di rendere più oggettiva e verificabile l'azione di polizia, dall'altro contribuiscono a ridefinire i confini della cittadinanza e a rafforzare forme di disuguaglianza sociale, incidendo in profondità sul rapporto tra individui, istituzioni e giustizia penale. Ovvero, la polizia predittiva, trasformando le modalità attraverso cui vengono esercitati il controllo e la sorveglianza, ridefinisce anche chi è considerato un "buon cittadino" o un soggetto "a rischio". I sistemi predittivi non operano nel vuoto. Si basano su dati preesistenti, raccolti in modo storicamente selettivo e spesso distorto. Questo significa che alcuni gruppi sociali – soprattutto minoranze razzializzate o persone che vivono in aree già fortemente sorvegliate – vengono più facilmente

[83] S. Brayne, *Big Data Surveillance: The Case of Policing*, cit.

etichettate come "a rischio", anche in assenza di comportamenti illeciti. La loro cittadinanza, pur formalmente piena, viene materialmente erosa, perché soggetta a una sorveglianza continua e a un trattamento differenziato. Con la *predictive policing*, non è più necessario "fare qualcosa" per attirare l'attenzione della polizia: può bastare trovarsi nel "profilo" sbagliato, in una rete sociale sorvegliata, o in un quartiere classificato come problematico. Questo sposta il baricentro della cittadinanza da un'idea di diritti universali a una logica di rischio calcolato, dove alcune biografie valgono meno di altre agli occhi del sistema. L'intervento poliziesco anticipato basato su *anticipatory evidence* non è solo una misura di sicurezza, ma diventa un dispositivo di esclusione: chi è "profilato" come minaccia viene preventivamente neutralizzato o sorvegliato, anche se formalmente non ha infranto la legge. Questo mina i principi fondamentali della cittadinanza democratica, basata sulla presunzione di innocenza e sull'uguaglianza di trattamento. Questo significa che il modello predittivo restringe i margini di esercizio della cittadinanza per alcuni soggetti, trasformando la relazione tra individuo e Stato da un rapporto fondato sui diritti a uno fondato sulla gestione del rischio[84].

4.4 Le prospettive degli operatori

Molte ricerche parlano degli strumenti di controllo data-driven, delle implicazioni che essi potrebbero avere in termini di discriminazione, privacy e giustizia sociale. Pochi arrivano ad interrogarsi su quali siano le opinioni degli operatori rispetto all'utilizzo di questi strumenti. Infatti, come avverte Brayne[85], è importante non dare per scontato che gli operatori utilizzino effettivamente questi strumenti, che sappiano come utilizzarli, o che li considerino utili o efficaci. Eppure, l'incidenza del fattore umano nell'utilizzo della tecnologia è ancora un elemento fondamentale da prendere in considerazione, poiché uno strumento predittivo si traduce in azione solo se effettivamente qualcuno decide di operare tale traduzione[86].

Sebbene in numero ridotto, alcuni studi si sono interrogati su questi aspetti.

Uno studio importante è quello di Neiva, Machado e Silva, che hanno condotto una revisione della letteratura empirica al fine di analizzare come gli operatori di polizia percepiscano l'impiego delle tecnologie data-driven nell'attività di polizia e nelle indagini criminali. Il punto di partenza dello studio è che esista una pro-

---

84 V. Galis, H. Oppen Gundhus, A. Vradis, *Critical Perspectives on Predictive Policing: Anticipating Proof?*, cit.

85 S. Brayne, *Predict and Surveil*, cit.

86 *Ibidem*.

spettiva ambivalente tra i professionisti del settore: se da un lato i big data rappresentano una risorsa promettente per potenziare le capacità di indagine, dall'altro sollevano interrogativi ancora irrisolti di natura etica, operativa e legale.

Attraverso una *scoping review*, gli autori hanno preso in esame 14 studi sulle opinioni degli operatori verso i big data pubblicati tra il 2015 e il 2022, in cui sono presenti sia atteggiamenti ottimistici che oppositivi verso i dispositivi data-driven[87].

Dalla revisione della letteratura emerge che molti operatori condividono un atteggiamento positivo nei confronti dei big data e ne sottolineano la capacità di accrescere l'efficienza e l'obiettività del lavoro di polizia. Considerano la tecnologia un mezzo in grado di migliorare la previsione dei reati, la valutazione dei rischi e le indagini, grazie alla possibilità di integrare e analizzare enormi quantità di dati. Evidenziano come l'analisi dei big data favorisca il riconoscimento di schemi ricorrenti, l'ottimizzazione delle risorse e l'individuazione di collegamenti tra casi e autori di reato. Alcuni professionisti hanno posto l'accento sul valore di tali strumenti nel sostenere il passaggio da un approccio di polizia reattivo a uno proattivo, in particolare attraverso modelli predittivi basati su dati provenienti dai social media, da informazioni geospaziali e da strumenti di sorveglianza. Inoltre, associano il ricorso ai big data a una progressiva "scientificazione" del lavoro di polizia, grazie all'introduzione di approcci data-driven nei processi decisionali. Osservano poi come tale tecnologia migliori l'interoperabilità tra banche dati istituzionali, favorendo la creazione di sistemi centralizzati che rafforzano l'attività di intelligence e consentono risposte in tempo reale. Alcuni funzionari europei, ad esempio, hanno evidenziato il ruolo dei big data nella risoluzione di *cold cases*, grazie a banche dati del DNA interoperabili e all'integrazione di diverse tipologie di dataset a supporto della cooperazione transnazionale di polizia. Accanto a questo ottimismo, non mancano tuttavia posizioni critiche e preoccupazioni. Una delle principali obiezioni riguarda i *bias* e gli errori insiti nelle tecnologie di big data. Sottolineano che il big data non costituisce uno strumento neutrale, ma riflette processi di categorizzazione e decisione umani. Temono quindi che si riponga un'eccessiva fiducia nelle tecnologie. Un ulteriore nodo problematico concerne la carenza di regolamentazione sull'uso dei big data nell'ambito delle attività di polizia, con conseguenti implicazioni per la privacy, la sicurezza dei dati e il rischio di abusi. Diversi professionisti hanno richiamato l'attenzione sull'assenza di quadri normativi solidi per regolare la raccolta, l'analisi e la condivisione delle informazioni, con il rischio che diritti fondamentali vengano violati. Alcuni studi hanno inoltre sottolineato i rischi di discriminazione genetica derivanti dall'uso dei dati del DNA a fini predittivi, con la possibilità di accuse infondate basate su predisposizioni genetiche.

---

87 L. Neiva, H. Machado, S. Silva, *The views about Big Data among professionals of police forces*, cit.

Altri studi mettono in luce che all'atto pratico alcuni agenti di polizia resistono alle nuove tecnologie. Nella ricerca *Pre-crime and policing of migrants: Anticipatory action meets management of concerns*, Gundhus e Jansen hanno analizzato l'implementazione in Norvegia dell'"Operazione Migrante", un progetto nazionale avviato nel 2015 per affrontare le sfide criminali connesse all'aumento della migrazione. Lo studio, basato su interviste qualitative a personale dell'intelligence e a soggetti istituzionali, ha messo in evidenza una notevole resistenza all'uso della tecnologia da parte degli operatori. Sebbene strumenti di *predictive policing* e sistemi data-driven fossero stati introdotti per facilitare azioni preventive, molti agenti si sono mostrati scettici e riluttanti rispetto alla loro piena adozione. Le principali resistenze hanno riguardato l'affidabilità dei dati – spesso incompleti o obsoleti –, la perdita nella discrezionalità del giudizio, ritenuto essenziale per un'azione di polizia efficace, e la percezione che la tecnologia imponesse priorità operative scollegate dalle realtà sul campo. Lo studio ha inoltre evidenziato carenze nella formazione e nella comprensione dei meccanismi algoritmici, che hanno limitato la capacità degli operatori di confrontarsi criticamente con gli strumenti tecnologici. Questa resistenza riflette più in generale le sfide culturali e istituzionali nel processo di integrazione delle nuove tecnologie nelle pratiche tradizionali di polizia, nelle quali l'esperienza e l'intuizione continuano a essere ampiamente valorizzate[88].

Pur riconoscendo le promesse di maggiore efficienza, di migliore allocazione delle risorse e di accresciute capacità predittive, diversi fattori alimentano lo scetticismo e la riluttanza verso le forme di controllo data-driven tra gli agenti. Una fonte cruciale di resistenza risiede nella diffidenza verso gli output algoritmici, percepiti come astratti e distanti dalle realtà operative. A ciò si aggiungono timori legati alla perdita di autonomia decisionale e al ridimensionamento del potere discrezionale e del giudizio professionale. Anche in questo caso, le lacune formative rappresentano una barriera significativa: la scarsa familiarità con la logica e il funzionamento degli strumenti di big data generano disorientamento e resistenze. Preoccupazioni etiche, infine, aggravano ulteriormente tali tensioni, poiché gli agenti manifestano disagio rispetto alle implicazioni per la privacy e al rischio di rafforzare i pregiudizi insiti nei dati storici. Si tratta, dunque, di resistenze che riflettono più ampi problemi culturali e istituzionali, in un contesto in cui intuizione ed esperienza restano fortemente valorizzate[89].

---

88 H.O.I. Gundhus, P.T. Jansen, *Pre-crime and policing of migrants: Anticipatory action meets management of concerns*, in *Theoretical Criminology*, 2019, pp. 1-20.

89 S. Brayne, *Big Data Surveillance: The Case of Policing*, cit.

5. Polizia e controllo data-driven in Italia e UE

5.1 L'AI-Act e la polizia predittiva in Europa

L'utilizzo di tecnologie data-driven e l'impiego di algoritmi e big data nelle pratiche di polizia ha avuto origine negli Stati Uniti, dove si è sviluppata una letteratura particolarmente ampia e critica sul tema. Per questa ragione, nella prima parte del presente lavoro abbiamo dato ampio spazio ai modelli di polizia predittiva statunitensi, che rappresentano la matrice teorica e operativa di molte esperienze successive. Tuttavia, nel corso degli anni, queste strategie si sono progressivamente diffuse anche in altri contesti nazionali, Europa compresa.

Anche in Europa si è così sviluppata una letteratura volta a interrogarsi sul funzionamento di questi strumenti e sulle implicazioni del loro utilizzo. Tuttavia, l'implementazione delle tecnologie data-driven nello spazio europeo è accompagnata da sfide complesse di ordine etico, giuridico e operativo, che impongono una riflessione critica sulla loro legittimità e sostenibilità democratica.

Il quadro giuridico europeo in materia di intelligenza artificiale applicata alla sicurezza pubblica e alla polizia predittiva si articola principalmente attorno a due strumenti normativi centrali: la direttiva UE 2016/680 cd. LED (Law Enforcement Directive), e il più recente Regolamento (UE) 2024/1689, noto come AI Act.

La Direttiva LED disciplina il trattamento dei dati personali da parte delle autorità di polizia e giudiziarie per finalità di prevenzione, indagine, accertamento e perseguimento di reati, nonché per l'esecuzione di sanzioni penali. Mira a garantire un elevato livello di protezione dei dati personali nel settore della giustizia penale, bilanciando la necessità di sicurezza pubblica con il rispetto dei

diritti fondamentali degli individui. La Direttiva stabilisce i principi generali del trattamento, che comprendono: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione e sicurezza. Rientrano nel suo ambito anche dati particolarmente sensibili come quelli biometrici, genetici o sanitari che richiedono misure di tutela rafforzate. La LED vieta le decisioni basate unicamente su trattamenti automatizzati che producano effetti giuridici o incidano in modo significativo sull'interessato, salvo che siano previste garanzie adeguate e l'intervento umano sia assicurato. Gli interessati hanno diritto di accesso, rettifica e cancellazione dei dati personali, sebbene tali diritti possano essere limitati per esigenze di sicurezza pubblica o per il buon esito delle indagini. La Direttiva impone inoltre obblighi di sicurezza, di documentazione e di cooperazione con le autorità di controllo, come il Garante per la protezione dei dati personali. In generale, la LED mira a garantire che il trattamento dei dati personali da parte delle autorità penali sia necessario e proporzionato, sottoposto a controlli indipendenti e pienamente compatibile con la Carta dei diritti fondamentali dell'Unione europea[1].

L'AI Act, invece, introduce una regolamentazione di settore finalizzata a disciplinare lo sviluppo, la messa in commercio e l'uso dei sistemi di intelligenza artificiale nell'Unione europea secondo un approccio basato sul rischio. In particolare, facendo tesoro anche di tutte le critiche che si sono sviluppate nei confronti dei sistemi di polizia predittiva negli Stati Uniti, l'AI Act ha introdotto un sistema di classificazione secondo cui alcune tecnologie sono vietate, altre sono considerate ad alto rischio, e altre devono semplicemente ottenere una certificazione (il regolamento distingue tra pratiche vietate, sistemi ad alto rischio e sistemi a rischio limitato).

Tra le pratiche vietate rientrano, ad esempio, l'uso di sistemi di riconoscimento biometrico a distanza in tempo reale in spazi pubblici a fini di *law enforcement*, in quanto considerati una minaccia sproporzionata ai diritti fondamentali. Sono tuttavia ammesse delle deroghe. L'art. 5(1)(h) AI Act vieta l'uso di sistemi di riconoscimento facciale in tempo reale in spazi accessibili al pubblico, salvo tre eccezioni: ricerca mirata di vittime di reati specifici, come rapimenti o tratta di esseri umani; prevenzione di minacce gravi e imminenti, come attacchi terroristici; individuazione, localizzazione o identificazione di un sospettato di reati gravi, definiti secondo il diritto dell'UE o degli Stati membri. In tutti questi casi, l'uso deve essere autorizzato da un'autorità giudiziaria o da un'autorità

[1] Si veda I. Neroni Rezende, *Facial Recognition for Preventive Purposes: the Human Rights Implications of Detecting Emotions in Public Spaces*, in L. Bachmaier Winter, S. Ruggeri (a cura di), *Investigating and Preventing Crime in the Digital Era*, Cham, Springer, 2022, pp. 67-98.

competente, e deve rispettare i principi di necessità, proporzionalità e limitazione nel tempo e nello spazio[2]. Sono vietati anche i sistemi di tipo *person-based* che cercano di prevedere la probabilità che un individuo commetta un reato basandosi unicamente sulla sua profilazione. Ciò significa formulare previsioni sul comportamento criminale di un individuo esclusivamente sulla base di dati personali che descrivono chi è quella persona, senza considerare elementi oggettivi, contestuali o probatori. In questi casi, l'algoritmo si limita a elaborare informazioni come età, residenza, precedenti contatti con la polizia, affiliazioni sociali o caratteristiche della personalità, per attribuire un punteggio di rischio o classificare la "pericolosità" del soggetto. L'AI Act vieta espressamente queste pratiche, in quanto presentano rischi inaccettabili: violano la presunzione d'innocenza, espongono a discriminazioni sistemiche e non garantiscono trasparenza né controllo umano significativo.

Sono invece ammessi, ma sottoposti a una disciplina stringente, i sistemi classificati come ad alto rischio. Tra questi rientrano: 1) i sistemi *place-based*, come quelli volti a individuare aree urbane a rischio di criminalità; 2) i sistemi *person-based* condizionati al rispetto di requisiti normativi e non basati unicamente sulla profilazione, che possono essere utilizzati solo come supporto alla valutazione di un investigatore quando esistono già sospetti ragionevoli e dati concreti[3]; 3) i sistemi *suspect-based*, impiegati per indagini complesse, ad esempio per collegare tra loro crimini seriali e individuare possibili autori. Questi ultimi rappresentano una sottocategoria delle pratiche person-based e si caratterizzano per la costruzione di un profilo anonimo del possibile autore di reati seriali. A differenza dei sistemi che mirano a identificare direttamente individui specifici, questi modelli elaborano caratteristiche comportamentali e operative ricorrenti (modus operandi) per delineare un "tipo" di sospetto, che può poi essere confrontato con soggetti reali[4]. Queste tecnologie non sono vietate, ma comporta-

---

[2] Vedi E. Pietrocarlo, *La predictive policing nel regolamento europeo sull'intelligenza artificiale*, cit.

[3] I sistemi person-based ammessi sono quei modelli predittivi che, pur mirando a identificare soggetti potenzialmente coinvolti in attività criminali, non si basano esclusivamente sulla profilazione individuale. Al contrario, integrano la valutazione algoritmica con altri elementi oggettivi, contestuali e normativi. Questi sistemi sono ammessi solo se la profilazione non è l'unico criterio decisionale, se esiste una base giuridica esplicita che ne autorizza l'uso, e se sono previste garanzie procedurali, come il controllo umano significativo e la possibilità di contestazione da parte dell'interessato (dunque, i sistemi di predizione algoritmica non possono operare come black-boxes). In tal senso, i sistemi person-based sono ammessi quando non operano in modo automatico e discriminatorio, ma si inseriscono in un processo decisionale più ampio e regolato, volto a tutelare i diritti fondamentali dell'individuo. Si veda E. Pietrocarlo, *La predictive policing nel regolamento europeo sull'intelligenza artificiale*, cit.

[4] Pietrocarlo evidenzia il rischio che, pur partendo da un profilo anonimo, questi strumenti possano generare effetti discriminatori o restrizioni indebite se utilizzati per restringere il campo dei sospetti in modo automatizzato. *Ibidem*.

no rischi significativi per i diritti fondamentali. Per questo il legislatore europeo ha imposto requisiti severi (c.d. 'requisiti essenziali), che includono la qualità e rappresentatività dei dati, la supervisione umana, la trasparenza algoritmica, l'adozione di misure di accountability e la realizzazione di valutazioni d'impatto sui diritti fondamentali prima della loro implementazione.

Accanto a questa distinzione, l'AI Act prevede alcune deroghe eccezionali. In circostanze straordinarie – ad esempio per ragioni di sicurezza pubblica particolarmente rilevanti – gli Stati membri possono autorizzare temporaneamente l'uso di sistemi basati esclusivamente sulla profilazione. Queste deroghe, però, devono avere una durata limitata e rispettare precise garanzie giuridiche e procedurali, così da ridurre al minimo i rischi per i diritti dei cittadini. Proviamo a chiarire meglio con degli esempi: un sistema vietato sarebbe quello che attribuisce automaticamente a un individuo un "punteggio di rischio criminale" basandosi solo sul fatto che vive in un quartiere considerato problematico, ha precedenti denunce o appartiene a un determinato gruppo sociale. In questo caso, la persona verrebbe trattata come potenzialmente pericolosa a prescindere da comportamenti concreti, un approccio che contrasta con la presunzione di innocenza e apre la strada a discriminazioni sistematiche. Un sistema ad alto rischio, invece, potrebbe essere un software che analizza i dati sui furti d'auto in una città e segnala che in una determinata zona il fenomeno è in crescita nelle ore notturne. La polizia può decidere di rafforzare i controlli in quell'area, utilizzando l'informazione come supporto operativo. Allo stesso modo, un sistema di tipo *suspect-based* può aiutare a collegare tra loro più rapine compiute con modalità simili, suggerendo che possano essere opera dello stesso autore. In questi casi la tecnologia non sostituisce il giudizio umano, ma lo affianca, fornendo indicazioni utili che devono comunque essere valutate criticamente dagli investigatori. Un sistema di riconoscimento facciale può ricadere sia tra le tecnologie vietate sia tra quelle ad alto rischio, a seconda delle modalità di utilizzo. È vietato il riconoscimento facciale utilizzato in tempo reale negli spazi pubblici, per identificare indiscriminatamente chiunque passi davanti a una telecamera, senza un sospetto specifico e senza limiti di tempo o luogo. Questo uso è vietato perché equivale a una forma di sorveglianza di massa, incompatibile con la dignità umana, la privacy e la libertà di movimento dei cittadini. Ad esempio, installare sistemi di riconoscimento facciale in tutte le stazioni ferroviarie per controllare automaticamente i volti di milioni di persone sarebbe vietato. È considerato ad alto rischio il riconoscimento facciale impiegato in modalità post-evento e in contesti mirati, cioè quando viene usato per confrontare un volto ripreso da una telecamera durante un crimine con le immagini contenute in un archivio (come la banca dati delle fotografie segnaletiche), al fine di identificare un sospetto già

collegato a un'indagine specifica. In questo caso, la tecnologia è soggetta a vincoli di accuratezza, trasparenza, supervisione umana, tracciabilità delle decisioni e possibilità di contestazione.

L'AI Act vieta anche pratiche di *scraping* massivo di immagini prese da internet o dai social media per creare banche dati di riconoscimento facciale. Questa attività è considerata vietata perché implica una raccolta indiscriminata di dati biometrici da persone che non hanno dato alcun consenso, genera banche dati enormi e non controllate, che possono essere usate per sorveglianza di massa e compromette in modo grave il diritto alla privacy e alla protezione dei dati personali. Ad esempio, se una forza di polizia scaricasse milioni di foto dai profili social per alimentare un sistema di riconoscimento facciale, quel sistema sarebbe vietato dall'AI Act. Diverso, invece, è il caso in cui la polizia utilizzi immagini raccolte in modo legittimo e circoscritto (ad esempio foto segnaletiche già presenti nei propri archivi ufficiali). In questo scenario, il riconoscimento facciale non è vietato, ma è comunque considerato un sistema ad alto rischio.

L'approccio europeo, dunque, si caratterizza per una tensione tra l'apertura all'uso di tecnologie innovative in ambito di sicurezza e la necessità di preservare la centralità dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'UE e dalla Convenzione europea dei diritti dell'uomo. Tale impostazione segna una differenza rispetto ad altri contesti normativi, privilegiando un controllo *ex ante* sull'impiego dell'AI, in cui la privacy e la dignità individuale costituiscono parametri insuperabili per la legittimità delle pratiche di sorveglianza predittiva.

5.2 La ricerca su big data e polizia in Europa

Esistono diversi software di polizia predittiva in uso nei Paesi europei. Vediamone alcuni e i problemi che sollevano, molti dei quali sono già emersi nei capitoli precedenti. Nei Paesi germanofoni (Germania e Svizzera) il software PRECOBS (Pre-Crime Observation System) utilizza dati storici sui furti in appartamento, individuando ricorrenze spaziali e temporali (*near repeats*), per segnalare aree ad alto rischio e orientare pattugliamenti e altri interventi di prevenzione. Oggi è impiegato da diverse autorità di polizia e alcune stanno testando una versione più evoluta, PRECOBS Enterprise, capace di aggiornare le previsioni in tempo reale e integrare nuove tipologie di dati. Più che introdurre un modo del tutto nuovo di pensare la sicurezza, PRECOBS rafforza pratiche già consolidate come l'intelligence e il cosiddetto calcolo del rischio: cioè quella prassi, già presente nella polizia tradizionale, che consiste nel valutare e mappare la probabilità di

futuri reati in specifici luoghi e momenti per decidere dove concentrare risorse e pattugliamenti. La novità sta nel fatto che questi processi, prima affidati soprattutto all'esperienza e all'analisi manuale, vengono ora automatizzati e accelerati da algoritmi statistici. Questi ultimi sono algoritmi "classici" di analisi statistica predittiva, non necessariamente "intelligenti": si basano su regole e modelli definiti a priori dagli sviluppatori. L'evoluzione in corso, però, guarda verso algoritmi di apprendimento automatico (autoapprendenti): sistemi capaci di adattarsi e migliorare da soli man mano che ricevono nuovi dati, senza che un programmatore debba ridefinire le regole ogni volta. Esempi tipici di questa categoria sono il machine learning e il deep learning. Questa transizione apre la strada a una logica più preventiva, in cui l'obiettivo diventa agire prima ancora che un reato possa verificarsi. Ne deriva una crescente *datafication* del lavoro di polizia, in cui l'analisi predittiva – da semplice supporto operativo – tende a diventare un elemento centrale della governance della sicurezza[5].

In Danimarca, a partire dal 2016, è stato adottato il sistema POL-INTEL, una versione personalizzata della piattaforma Gotham[6], sviluppata dalla società statunitense Palantir Technologies, già nota per le sue collaborazioni con agenzie come la CIA e la NSA. Il progetto si colloca pienamente nel paradigma dell'Intelligence-Led Policing (ILP), che privilegia approcci proattivi e basati su analisi sistematiche dei dati, piuttosto che risposte reattive a eventi già accaduti. Il sistema consente di integrare e visualizzare grandi quantità di dati provenienti da fonti eterogenee, offrendo strumenti avanzati come analisi di hotspot, segmentazioni temporali, analisi di reti sociali, nonché applicazioni di machine learning e deep learning. L'obiettivo dichiarato è quello di potenziare la capacità della polizia danese di anticipare e prevenire i reati, ottimizzando l'impiego delle risorse e intervenendo in modo mirato contro fenomeni come i furti seriali o le minacce terroristiche. Per raggiungere tali fini, POL-INTEL si basa sull'uso di dati storici sui reati, informazioni geografiche, dati di intelligence e pattern criminali estratti dai registri istituzionali. Sebbene POL-INTEL sia una specifica implementazione danese, la piattaforma Gotham su cui si fonda è già stata adottata in altri paesi, tra cui gli Stati Uniti e la Germania, confermando la crescente influenza internazionale delle soluzioni di *predictive policing* sviluppate da Palantir. Secondo Karlsson e Galis (2025), l'esperienza danese con POL-INTEL rivela con forza tanto le ambizioni quanto i limiti della polizia predittiva. Se da

[5] S. Egbert, S. Krasmann, *Predictive policing: not yet, but soon preemptive?*, in *Policing and Society*, 2020, 30(8), pp. 905-919.

[6] Palantir Gotham è una piattaforma di analisi dei dati sviluppata dall'azienda statunitense Palantir Technologies e ampiamente adottata da forze di polizia e agenzie governative in diversi paesi.

un lato il sistema è stato presentato come un progetto altamente innovativo, in grado di trasformare la polizia in un'organizzazione più razionale, scientifica e predittiva, dall'altro la sua implementazione ha generato una serie di criticità. Sono i rischi che abbiamo già incontrato. In primo luogo, l'opacità algoritmica: essendo basato su un'infrastruttura proprietaria sviluppata da un'azienda privata, POL-INTEL solleva dubbi di trasparenza, controllo democratico e accountability. In secondo luogo, l'uso intensivo di dati storici e di intelligence rischia di riprodurre *bias* preesistenti, legittimando forme di sorveglianza mirata che possono colpire in maniera sproporzionata gruppi già vulnerabili. A ciò si aggiunge la tensione tra le aspettative pubbliche di un "super-weapon" tecnologico e le difficoltà pratiche riscontrate nell'adattare un sistema così complesso alle esigenze quotidiane del lavoro di polizia[7].

Gotham è stato anche utilizzato dalle autorità danesi per anticipare potenziali minacce legate alla migrazione, combinando l'analisi di dati provenienti da banche dati poliziesche, registri migratori, fonti aperte e dati personali. Il sistema consente di identificare pattern sospetti, visualizzare connessioni tra individui, luoghi ed eventi e generare *alert* predittivi che guidano le decisioni operative. Questo approccio ha permesso di integrare tecnologie predittive in strategie di sicurezza che mirano a contenere i flussi migratori e prevenire rischi percepiti per l'ordine pubblico[8].

Un quadro simile, si riscontra anche in Norvegia, dove le autorità di polizia fanno uso di strumenti analitici per produrre analisi del rischio e report di intelligence finalizzati alla gestione dei fenomeni migratori. Ne parlano Gundhus e Jansen, ma senza riferimento a un software specifico. In questo caso, i dati utilizzati provengono da archivi interni della polizia e da fonti condivise da agenzie europee come Frontex, Europol e Interpol. L'obiettivo è quello di prevedere minacce potenziali, come il crimine organizzato, il terrorismo o disordini pubblici, e orientare di conseguenza l'allocazione delle risorse. Tuttavia, secondo gli autori, l'uso di tali strumenti contribuisce spesso a moltiplicare le incertezze piuttosto che risolverle, soprattutto quando le analisi si basano su indicatori imprecisi o speculativi. In entrambi i contesti, danese e norvegese, le tecnologie predittive vengono inserite in una logica precauzionale che valuta migranti e richiedenti asilo non sulla base di comportamenti passati documentati, ma in funzione di rischi potenziali futuri. Categorie generiche come "minori non ac-

[7] Karlsson, V. Galis, *POL-INTEL: Predictive policing and the politics of data integration in Denmark*, cit.

[8] H.O.I. Gundhus, P.T. Jansen, *Pre-crime and policing of migrants: Anticipatory action meets management of concerns*, cit.

compagnati", "individui instabili" o "gruppi vigilanti" rischiano di rafforzare stereotipi e sospetti, generando una conoscenza solo apparentemente oggettiva. In particolare, le rappresentazioni dei minori non accompagnati presentano un certo grado di ambivalenza: da un lato presentati come soggetti vulnerabili, dall'altro come potenziali minacce. Questi sistemi rischiano di stigmatizzare le persone migranti, legittimare pratiche coercitive e securitizzare ulteriormente le politiche migratorie[9].

In Norvegia sono vari i software che vedono l'utilizzo di tecnologia data-driven da parte delle forze di polizia. Uno di questi è il software Omnia, un sistema predittivo anch'esso creato dalla già nota società Palantir Technologies. L'obiettivo prevedeva di integrare una vasta gamma di dati – dagli indirizzi residenziali alle cartelle cliniche, dai dati di trasporto a condanne penali, fotografie e informazioni biometriche come il DNA – per potenziare la capacità delle forze dell'ordine di anticipare crimini e gestire in modo strategico la sicurezza pubblica[10]. Tuttavia, il progetto è stato interrotto dopo 11 anni di sviluppo e un investimento di circa 100 milioni di corone norvegesi. Il fallimento del progetto, sebbene le ragioni non siano del tutto chiaro, sembra si debba a vari fattori, non solo tecnici, come la carenza di dati adeguati, ma anche di natura sociale, come una certa incompatibilità con il contesto sociale norvegese, e pressioni da parte di organizzazioni per i diritti civili, preoccupate per il potenziale uso discriminatorio della tecnologia data-driven.

Un altro software è il Parabon Snapshot, che mira a prevedere i tratti somatici di una persona (colore della pelle, degli occhi, dei capelli) a partire dal suo DNA. Sviluppato da aziende private, può essere utilizzato per ricostruire l'aspetto fisico di sospetti ignoti quando il confronto diretto con profili già noti fallisce. Si tratta dunque di utilizzo dell'AI nella genetica forense, in particolare attraverso le tecnologie di DNA phenotyping. Secondo Kaufman, sebbene promettano di fornire nuove piste investigative, tali strumenti sollevano gravi questioni etiche, in quanto si basano su correlazioni genetiche soggette a interpretazioni arbitrarie, che rischiano di rafforzare stereotipi razziali e amplificare il rischio di profilazione discriminatoria. Inoltre, l'impiego di tratti fenotipici generali anziché dell'identificazione individuale introduce una svolta epistemologica nella polizia scientifica, che dal riconoscimento certo di un singolo soggetto si sposta verso previsioni probabilistiche basate su categorie di gruppo. Sempre in Norvegia, a Oslo, tra il 2019 e il 2021, è stato sviluppato il progetto

---

9 *Ibidem*.

10 M. Kaufmann, *AI in policing and law enforcement*, in *Handbook on Public Policy and Artificial Intelligence*, Cheltenham-Northampton, Edward Elgar Publishing, 2024, pp. 295-304.

KIBU (Crime Preventive Effort for Children and Young People). L'iniziativa era finalizzata a individuare precocemente giovani vulnerabili o potenzialmente inclini a condotte criminali future, così da predisporre interventi preventivi mirati. A tal fine, la polizia ha integrato banche dati interne (PAL STRASAK, PAL PO e Indicia) con strumenti di analisi quali Excel – impiegato per la pulizia e la strutturazione dei dati – e, soprattutto, con il software Analyst's Notebook (ANB), sviluppato dall'azienda i2 (IBM) e ampiamente diffuso a livello internazionale nei contesti di intelligence e *law enforcement*.

ANB è stato utilizzato per condurre analisi di rete e per visualizzare le connessioni tra individui, eventi e reati, facilitando così l'individuazione dei soggetti considerati a rischio. Il set di dati analizzato non comprendeva soltanto reati registrati e segnalazioni di incidenti, ma anche indicatori sociali e familiari quali la separazione o il divorzio dei genitori, precedenti penali in famiglia, problemi di abuso di sostanze, disturbi psichici o esperienze di violenza domestica. Come rilevano Erichsen e Gundhus, l'impiego di ANB e di tali indicatori ha introdotto elementi di innovazione rispetto alle pratiche investigative tradizionali, fornendo alle forze di polizia nuovi strumenti per la prevenzione giovanile. Tuttavia, questo approccio tende a generare processi di etichettamento: i giovani vengono classificati come "a rischio" non sulla base di reati effettivamente commessi, bensì in virtù di predizioni e correlazioni probabilistiche. Inoltre, poiché i registri di polizia includono frequentemente informazioni parziali, sospetti o segnalazioni non verificate, le valutazioni prodotte da ANB risultano suscettibili di *bias* e distorsioni. Ne deriva che, più che ridurre l'incertezza, tali tecnologie finiscono per riconfigurarla, offrendo un'apparenza di oggettività predittiva che lascia spazio a interpretazioni soggettive e potenzialmente discriminatorie[11].

Nel contesto olandese, uno degli strumenti più noti di polizia predittiva è il Crime Anticipation System (CAS), utilizzato dalla polizia dei Paesi Bassi. Il CAS è un sistema un po' diverso dagli altri, in particolare per le modalità con cui è stato prodotto. Infatti, è stato sviluppato internamente dalla polizia olandese, in collaborazione con il Ministero della Giustizia e della Sicurezza, e non da un'azienda privata. È stato implementato per supportare le pattuglie nel prevenire determinati reati, come furti in abitazione e furti con scasso, attraverso l'analisi statistica dei dati storici sul crimine. Il sistema combina dati di reati passati con localizzazione geografica, orari degli eventi e altre informazioni contestuali per identificare aree a rischio elevato, visualizzate su una mappa con

[11] P. Erichsen Skjevrak, H.O.I. Gundhus, *From personal archives to intelligence: Visibility and ignorance in forecasting "youth at risk"*, in V. Galis, H.O.I. Gundhus, A. Vradis (a cura di), *Critical Perspectives on Predictive Policing*, Cheltenham-Northampton, Edward Elgar Publishing, 2025, pp. 63-83.

"hotspots" evidenziati. Queste mappe vengono aggiornate quotidianamente per decidere dove dispiegare le risorse di polizia. Il CAS non è un software commerciale ed è stato sviluppato per essere usato esclusivamente nei Paesi Bassi, senza indicazioni di estenderne l'adozione ad altri paesi. La polizia olandese lo ha testato e applicato principalmente in aree urbane come Amsterdam e Utrecht. Dopo un'accoglienza iniziale entusiasta, il sistema è stato gradualmente ritirato in alcune zone, poiché accusato di scarsa efficacia, opacità nei criteri di funzionamento e possibili effetti discriminatori. In particolare, l'uso di dati storici rischiava di perpetuare pratiche di polizia già sbilanciate verso specifici quartieri o gruppi sociali, finendo per consolidare anziché ridurre le disuguaglianze.

A differenza dei software statunitensi – come PredPol, spesso sviluppati da aziende private e caratterizzati da algoritmi opachi – il CAS olandese si distingue per una progettazione pubblica e trasparente, frutto della collaborazione tra diverse istituzioni statali. Questo approccio "domestico" riflette una maggiore attenzione alla responsabilità democratica e al controllo pubblico; tuttavia, come abbiamo visto, non elimina le criticità connesse all'uso predittivo delle serie storiche di dati né le implicazioni sociali delle pratiche di sorveglianza algoritmica[12].

In Svezia è invece in uso il sistema STATUS. Quest'ultimo è stato sviluppato a partire dal 2005 e si è diffuso a livello nazionale a partire dal 2015. Si tratta di un sistema di supporto decisionale e analisi predittiva che non è stato creato *ex novo*, ma costruito come un ecosistema di applicazioni basate su due strumenti di business *analytics* prodotti dalla società svedese QlikTech: QlikView e QlikSense. QlikView, diffuso dagli anni '90, permette di integrare dataset differenti e di esplorarli in maniera interattiva grazie a un motore di associazioni che evidenzia connessioni non immediatamente visibili; QlikSense, introdotto in seguito, rappresenta la sua evoluzione, con un'interfaccia più intuitiva e funzionalità avanzate di *data storytelling*, *machine learning* e *predictive analytics*. Su questa infrastruttura tecnologica, la polizia ha costruito un sistema adattato alle proprie esigenze, capace di elaborare quotidianamente dati provenienti da diversi registri interni (RAR, STORM, DURTvå) senza salvarli in modo permanente. STATUS consente di condurre analisi geografiche, temporali e organizzative. Sul piano geografico, è possibile visualizzare i dati su mappe, identificando hotspot di criminalità nei quartieri e nei distretti; sul piano temporale, i dati possono essere disaggregati per giorni, settimane, mesi o anni, così da individuare possibili trend stagionali di alcuni reati o momenti specifici in cui essi ricorrono con maggiore frequenza; infine, sul piano organizzativo, il sistema permette

[12] M. Schuilenburg, M. Soudijn, *Big data policing in the Netherlands: The politics of unpredictability*, in *European Journal of Criminology*, 2023, 20(2), pp. 246-264.

di analizzare l'attività delle diverse unità e reparti, monitorando carichi di lavoro e allocazione delle risorse. Tutti i risultati vengono pubblicati su Intrapolis, l'intranet della polizia, così da essere accessibili in tempo reale a vari livelli dell'organizzazione, dagli analisti agli ufficiali di comando fino alle pattuglie operative.

Dal 2020 è stata pianificata la transizione a un nuovo sistema, denominato KUPOL, che integra lo Swedish Crime Harm Index (SCHI), con l'obiettivo di spostare l'attenzione dai semplici hotspot a veri e propri *harm-spots*, ossia aree in cui i reati hanno un impatto sociale particolarmente elevato. In altre parole, non conta soltanto il numero di reati registrati, ma anche il loro peso sulla comunità: ad esempio, una serie di piccoli furti ha un impatto diverso rispetto a episodi di violenza grave o di crimine organizzato. Lo SCHI permette quindi di distinguere tra reati ad alta frequenza ma a basso impatto e reati meno frequenti ma molto più dannosi, così da orientare meglio le risorse della polizia verso le situazioni che creano maggiore sofferenza sociale e insicurezza collettiva.

Il caso di STATUS e la sua evoluzione rappresenta un ottimo esempio di come la polizia predittiva non vada interpretato solo come una questione di efficienza tecnologica, ma come una pratica di governance che intreccia dati, valori sociali e strategie di sicurezza. Questi strumenti data-driven non sono mai neutri, ma riflettono e riproducono le priorità organizzative e politiche della polizia che li adotta. La transizione a KUPOL e l'introduzione dello *Swedish Crime Harm Index* (SCHI) rendono ancora più evidente che le scelte su cosa considerare un "reato ad alto impatto sociale" non sono solo questioni statistiche, ma decisioni normative e politiche[13].

Uno degli esempi più significativi di come la polizia predittiva si stia intrecciando con le logiche della sorveglianza urbana contemporanea è il caso del riconoscimento facciale in tempo reale (Live Facial Recognition, LFR) nel Regno Unito. Il LFR consiste nell'integrazione di algoritmi di riconoscimento biometrico con le reti di telecamere CCTV installate in spazi pubblici. Il sistema cattura in tempo reale i volti dei passanti, li traduce in dati geometrici (distanze tra occhi, naso, bocca, ecc.) e li confronta con database preesistenti di immagini, come schedari di polizia o archivi biometrici nazionali. A differenza del riconoscimento "uno-a-uno" utilizzato in contesti come gli aeroporti o i telefoni cellulari, quello urbano è un riconoscimento "uno-a-molti": ogni volto viene confrontato simultaneamente con migliaia di altri. In caso di corrispondenza, il sistema genera un *match* che può attivare un intervento immediato delle pattuglie di polizia. Il LFR è stato introdotto nel Regno Unito

[13] G. Mattes, *Predictive policing in Sweden*, in V. Galis, H.O.I. Gundhus, A. Vradis (a cura di), *Critical Perspectives on Predictive Policing*, cit., pp. 165-183.

con il supporto di aziende private specializzate in software biometrici, come Visionics e Facematcher, ed è oggi gestito come parte dell'infrastruttura di sorveglianza pubblica. La sua applicazione è giustificata dalle autorità come strumento per identificare criminali ricercati, prevenire atti terroristici o aumentare la percezione di sicurezza nelle città. Tuttavia, le criticità sono numerose: studi indipendenti hanno mostrato tassi di errore elevati, con numerosi "falsi positivi" (innocenti scambiati per sospetti) e "falsi negativi" (criminali non riconosciuti); gli algoritmi presentano *bias* razziali e di genere, risultando meno accurati nel riconoscere donne e persone con la pelle scura; il LFR opera in un'area grigia dal punto di vista normativo, senza un chiaro quadro giuridico che ne regoli l'uso e con frequenti contestazioni da parte di ONG e gruppi per i diritti civili; la capacità del sistema di analizzare automaticamente i volti di chiunque attraversi un'area sorvegliata rappresenta una forma di sorveglianza indiscriminata, che mina i principi di proporzionalità e di libertà individuale[14].

Secondo Papada e Vradis, il LFR non è soltanto uno strumento tecnico, ma un dispositivo politico e culturale che ridefinisce i confini tra sicurezza e libertà, tra cittadinanza e sospetto, contribuendo a normalizzare un modello di città in cui la sorveglianza costante è percepita come inevitabile e naturale, con conseguenze a lungo termine per la percezione pubblica della sicurezza e per la definizione stessa di cittadinanza.

5.3 La polizia predittiva in Italia

Anche in Italia esistono esperienze di polizia predittiva, sebbene le informazioni disponibili siano limitate e sebbene non siamo certi che in questo momento siano in uso. Tali esperimenti appaiono tuttavia differenti da quelli sviluppati in altri paesi, in particolare negli Stati Uniti. In Italia, infatti, la previsione del crimine sembra basarsi quasi esclusivamente su dati prodotti dalla stessa polizia, integrando in maniera limitata altre tipologie di informazioni. Appaiono quindi diversi dai sistemi che adottano software che rendono interoperabili grandi quantità di dataset eterogenei, che consentono ricerche trasversali e che finiscono così per includere nelle operazioni di controllo, prevenzione e indagine anche dati originariamente raccolti per finalità diverse dalla giustizia e persino informazioni su persone che non hanno commesso né sono sospettate di alcun reato. Andiamo quindi a vedere nello specifico quali

[14] E. Papada, A. Vradis, *The birth of spatial transgression*, cit.

sono i sistemi di polizia predittiva o, più in generale, di polizia e utilizzo dei big data presenti in Italia.

5.3.1 Key crime

Tra le esperienze più rilevanti di applicazione della polizia predittiva in Italia merita particolare attenzione KeyCrime, un sistema nato all'interno della Polizia di Stato e successivamente sviluppato anche in collaborazione con soggetti privati[15]. Attivo dal 2008, rappresenta uno degli esempi pionieristici di polizia predittiva in Italia, insieme al software XLaw.

Il progetto prende avvio presso la Questura di Milano, grazie all'iniziativa di Mario Venturi, allora agente della Polizia di Stato, in un periodo in cui la città è colpita da un'ondata di rapine, in particolare ai danni di farmacie. L'idea di Venturi è quella di costruire uno strumento capace di raccogliere e analizzare in maniera sistematica i dati relativi a ogni rapina commerciale, per individuare schemi ricorrenti e sequenze criminali.

Il software elabora una quantità molto ampia di micro-dati (circa 11.000 variabili per ciascun evento): dal luogo e orario del reato alle modalità del colpo, dalle caratteristiche fisiche e dall'abbigliamento dell'autore fino al tipo di arma o di veicolo utilizzato. Vengono integrate anche informazioni provenienti da testimoni, raccolte tramite questionari standardizzati, o estrapolate da immagini di sorveglianza. Grazie a tecniche di *crime linking*, il sistema è in grado di confrontare i dati e riconoscere correlazioni tra episodi attribuibili allo stesso autore o gruppo criminale, anticipando la possibile evoluzione spazio-temporale dei reati e orientando così la pianificazione operativa delle pattuglie[16].

Un aspetto importante è che KeyCrime non sostituisce l'analisi umana, ma la affianca: l'algoritmo propone collegamenti e ipotesi, che devono essere valutati, confermati o scartati da chi poi prenderà decisioni operative[17].

L'evoluzione del sistema in ambito imprenditoriale ha portato alla nascita di DELIA (*Dynamic Evolving Learning Integrated Algorithm*), piattaforma gestita da un'azienda privata, che mantiene la stessa logica di supporto decisionale senza automatizzare l'ultima parola.

---

15 D.E. Pietrocarlo, *La predictive policing nel regolamento europeo sull'intelligenza artificiale*, in *La Legislazione Penale*, 2024, pp. 1-35.

16 G. Mastrobuoni, *Crime is Terribly Revealing: Information Technology and Police Productivity*, in *The Review of Economic Studies*, 2020, 87 (6), pp. 2727-2753

17 V. Cinelli, *Crime prevention and predictive analysis: the Italian case*, Agenfor Media, 2020, https://www.agenformedia.com/wp-content/uploads/2020/10/Technology1_VCinelli.pdf.

Dal punto di vista dei dati impiegati, KeyCrime si basa sulle informazioni a disposizione della polizia: denunce, verbali, rapporti investigativi. Tra queste rientrano dettagli sensibili come l'etnia o l'accento degli autori, spesso desunti da testimonianze. Secondo un report dell'Osservatorio Amministrazione Automatizzata (OAA), proprio l'uso di queste variabili costituisce uno dei principali rischi di *bias* e discriminazione: non è chiaro come tali informazioni vengano raccolte, validate e filtrate[18]. Questa critica è interessante perché, nonostante il sistema utilizzi dati prodotti dalla polizia, non è detto che questi dati non siano parziali e gravati da pregiudizi.

I rischi di discriminazione e pregiudizio esistono anche se il sistema riconosce una forte autonomia decisionale alla componente umana, cui spetta la decisione finale – che lo rende un sistema sicuramente migliore di altri. Persiste infatti una certa opacità nel funzionamento del software (il problema della "black box"). Inoltre, «le informazioni a cui il sistema è stato esposto per "conoscere" e modellare il fenomeno consistono nello storico dei reati codificati dalla polizia, dati che dipendono da come i crimini sono stati registrati e codificati, e che influenzano le predizioni future del sistema»[19].

Tuttavia, nel 2024 la società produttrice di KeyCrime è stata liquidata. L'entrata in vigore dell'AI Act ha reso incerto il futuro del software, che rischiava di essere classificato tra le tecnologie vietate, poiché in parte assimilabile a un sistema *person-based* basato su profilazione. L'ideatore ha sostenuto che si trattasse di un software *suspect-based*, destinato a risolvere indagini a partire da prove concrete e non a svolgere profilazione. Tuttavia, la necessità di ottenere una certificazione e l'incertezza dei tempi hanno reso insostenibile la prosecuzione del progetto. I fondatori hanno denunciato la lentezza nella certificazione ai sensi dell'AI Act, che ha alimentato incertezze sul futuro del progetto[20].

Questa vicenda appare particolarmente interessante anche perché il progetto Giove, avviato dal Ministero dell'Interno nel 2020, si ispira in parte proprio a KeyCrime, configurandosi come sua possibile evoluzione. Resta dunque aperto l'interrogativo su quale sarà il destino di Giove in un quadro giuridico che ha portato al fallimento del suo predecessore.

---

[18] Privacy Network, *Amministrazione automatizzata. Report 2024/2025*, https://media.privacynetwork.it/privacynetwork/uploads/2025/05/report-osservatorio-OAA.pdf, pp. 51-54.

[19] Privacy Network, *Amministrazione automatizzata*, cit., p. 52.

[20] M. Bizzini, *The Rise and Fall of a Predictive Policing Pioneer*, AlgorithmWatch, 2024, https://algorithmwatch.org/en/predictive-policing-pioneer-keycrime; A.D. Signorelli, *Perché la più avanzata startup italiana di polizia predittiva è sull'orlo del baratro*, in *Wired Italia*, 31 gennaio 2024, https://www.wired.it/article/polizia-predittiva-keycrime-startup-ai-act.

5.3.2 Giove

Giove è un sistema di polizia predittiva sviluppato in Italia per supportare le attività investigative, in particolare la prevenzione e repressione di reati a forte impatto sociale come furti, rapine, truffe, molestie e violenze sessuali[21]. Realizzato a partire dal 2020 dal Dipartimento di Pubblica Sicurezza del Ministero dell'Interno, trae le sue basi dal precedente software KeyCrime (in uso già dal 2008).

Proprio come Keycrime, il funzionamento di Giove si basa su un algoritmo di *crime linking*: analizzando dati come orario, luogo e modalità dei crimini commessi, Giove identifica serie potenziali di reati collegati alla stessa persona o gruppo. L'obiettivo è suggerire alle questure dove concentrare le risorse, indicando con maggiore efficienza momenti e luoghi a rischio.

Proprio come Keycrime, il sistema è pensato come un supporto tecnico all'indagine e non come strumento giudiziario autonomo. Ovvero, le decisioni finali rimangono in capo agli operatori. Le informazioni raccolte includono dati sulle denunce (comportamenti, elementi contestuali, video, foto, modalità della commissione del reato).

Le preoccupazioni e i rischi legati all'utilizzo di Giove sono quelle che abbiamo oramai imparato a conoscere: il rischio di *bias* algoritmici e la non trasparenza del sistema, inclusi gli interrogativi su quale banche dati verranno usate; di fronte a questo, il ruolo del Garante della Privacy è ancora insufficiente[22]; inoltre, si teme che le previsioni possano diventare elementi pre-probatori o addirittura giustificativi di misure cautelari, oltrepassando il confine tra ausilio tecnico e giudizio umano – un tema già inserito nelle raccomandazioni dell'Unione Europea per l'IA responsabile[23].

Giove è stato sottoposto a una interrogazione parlamentare depositata il 13 giugno 2023 al Senato da Filippo Sensi come primo firmatario. L'interrogazione, rivol-

---

21 Pegasoft, *Polizia predittiva, il software Giove prevedrà reati e omicidi*, Pegasoft S.r.l., 2023, https://www.pegasoftsrl.it/polizia-predittiva-il-software-giove-prevedra-reati-e-omicidi.

22 F. Ongaro, B. Simonini, *Software italiano Giove per la polizia predittiva: Pro e contro*, in *Agenda Digitale*, 5 settembre 2023, https://www.agendadigitale.eu/documenti/giustizia-digitale/ia-in-polizia-e-giustizia-predittiva-opportunita-e-rischi-del-software-italiano-giove.

23 E. Rosso, *Cosa sappiamo di Giove, l'algoritmo con cui la polizia italiana vuole prevedere i reati*, in *Fanpage.it*, 7 giugno 2023, https://www.fanpage.it/innovazione/tecnologia/cosa-sappiamo-di-giove-lalgoritmo-con-cui-la-polizia-italiana-vuole-prevedere-i-reati; M. Castigli, *L'Italia fa già "polizia predittiva" ed è ad "alto rischio" ma non vietata dall'UE: ecco perché*, in *Cybersecurity360*, 19 giugno2023, https://www.cybersecurity360.it/news/litalia-fa-gia-polizia-predittiva-e-ad-alto-rischio-ma-non-vietata-dallue-ecco-perche.

ta al Ministro dell'Interno e rimasta ad ora senza risposta, pone importanti interrogativi, in linea con i dubbi espressi dalla letteratura sul tema. Sensi, infatti, chiede:

> a) quali interventi intenda mettere in atto per introdurre il sistema Giove in Italia, se esistano altri *software* di questo tipo già in uso o dei quali si prospetta l'utilizzo; b) quali aziende siano state coinvolte nella definizione di questa tecnologia, della sua implementazione e del suo sviluppo; c) quale sia lo stato dell'arte della interlocuzione con il Garante per la protezione dei dati personali in ordine a una valutazione di impatto che l'introduzione di questo sistema comporterebbe; c) quale tipo di dati e quali *batch* si intenda utilizzare per andare a comporre la memoria operativa del sistema; d) che livello di individuazione sia possibile e ottenibile senza violare la *privacy* dei soggetti; e) quali siano gli effetti anche sull'urbanistica delle città alla prova di una capacità così penetrante e intrusiva di profilazione delle persone e dei comportamenti[24].

5.3.3 Xlaw e Pelta Suite

Xlaw è un software di polizia predittiva originariamente concepito presso la Questura di Napoli, nei primi anni 2000 e successivamente sviluppato da un'impresa privata. Si configura come un sistema *place-based* che, attraverso tecniche di *machine learning* e *deep learning*, analizza sia dati relativi a reati predatori urbani sia a variabili socio-economiche e demografiche[25]. L'obiettivo è individuare le aree urbane considerate maggiormente a rischio in specifici intervalli temporali, generando allarmi predittivi georeferenziati che permettono di orientare le strategie di controllo del territorio da una logica reattiva a una preventiva[26].

Il sistema, progettato e sviluppato dall'ispettore di polizia Elia Lombardo, è stato sperimentato in via operativa dalla Polizia di Stato a partire dal 2004 a Napoli e, dal 2013, esteso a città come Salerno, Prato, Parma, Modena e Venezia. Tra il 2013 e il 2021 la sperimentazione ha interessato anche altre realtà urbane, tra cui Trieste, Livorno, Bari, Catania e Trento[27]. Secondo l'azienda produttrice, i dati raccolti indicherebbero un calo del 39% dei reati nelle aree monitorate, ma tali risultati non sono stati verificati da soggetti indipendenti.

Nel 2021, Xlaw è stato acquisito da XServizi, che ne ha sviluppato l'evoluzione commerciale denominata *Pelta Suite*. Questa comprende due soluzioni di-

---

[24] Senato della Repubblica, *Legislatura 19ª – Atto di Sindacato Ispettivo n. 3-00499*, 13 giugno 2023, https://www.senato.it/show-doc?id=1378767&leg=19&tipodoc=Sindisp.

[25] D.E. Pietrocarlo, *La predictive policing nel regolamento europeo sull'intelligenza artificiale*, cit.

[26] M. Gialuz, S. Quattrocolo, *AI and the administration of criminal justice in Italy (A-01-23)*, in *Penal*, 2023, https://www.penal.org/sites/default/files/files/A-01-23.pdf.

[27] Privacy Network, *Amministrazione automatizzata*, cit.

stinte: *Pelta Urban Security*, destinata alle forze di polizia, e *Pelta GDO&Retail*, rivolta invece ad attività commerciali.

Dal punto di vista tecnico, Xlaw elabora dati contenuti in denunce e registri della polizia, senza riferirsi a individui specifici, ma con l'obiettivo di individuare schemi di comportamento criminale. Con *Pelta Suite* questo approccio è stato ulteriormente raffinato: il sistema lavora infatti su due strati di dati. Il primo riguarda i cosiddetti *big data* di contesto, cioè informazioni sugli eventi urbani rilevanti come arrivi di treni e navi, grandi manifestazioni o flussi di mobilità, utilizzati per costruire una sorta di "città virtuale". Il secondo strato integra invece i dati forniti dalla polizia, come denunce e registri criminali, sempre in forma non riferibile a individui specifici, per identificare modelli ricorrenti di comportamento criminale. L'interazione tra questi due livelli consente al software di simulare e prevedere i rischi di illegalità diffusa con un livello di dettaglio più sofisticato[28]. L'obiettivo è di anticipare eventi criminosi e ottimizzare l'impiego delle forze dell'ordine o dei responsabili della sicurezza privata.

Dal 2021 *Pelta Urban Security* è stata testata in alcune città italiane, tra cui Caorle (Veneto) e Signa (Toscana). Nel Comune di Caorle (Venezia), il software è stato personalizzato per prevenire furti, atti vandalici e fenomeni di degrado urbano, soprattutto durante i periodi di alta affluenza turistica. Un secondo progetto pilota ha riguardato il Comune di Signa (Firenze), dove la piattaforma è stata integrata nelle strategie di sicurezza territoriale a partire dal gennaio 2022. In questo contesto, l'attivazione del sistema è stata accompagnata da percorsi formativi rivolti al personale della polizia locale, curati direttamente da XServizi[29].

Dal punto di vista tecnico, Pelta Suite elabora dati socio-urbani, cronologici e ambientali tramite modelli di *machine learning*, producendo mappe del rischio consultabili sia dalla centrale operativa sia dagli agenti sul campo.

Il sistema ha ottenuto il brevetto nel 2022 e una validazione operativa da parte della Direzione Centrale Anticrimine del Dipartimento di Pubblica Sicurezza.

5.3.4 Vigilium

Vigilium rappresenta uno dei primi esempi italiani di piattaforma predittiva specificamente pensata per la sicurezza urbana. È stato inizialmente sperimentato nella

[28] *Ibid.*

[29] *Ibid.*; *Pelta per la sicurezza urbana a Signa*, https://www.pelta.it/notizie/comunicati-stampa/pelta-sicurezza-urbana-a-signa; *Speciale IA e polizia predittiva – Format informativo*, https://www.pelta.it/speciale-ia-e-polizia-predittiva.

città di Trento, sotto il coordinamento del gruppo di ricerca *eCrime* della Facoltà di Giurisprudenza dell'Università di Trento, in collaborazione con la Questura, il Centro ICT della Fondazione Bruno Kessler e il Comune. Successivamente, il sistema è stato adottato nel 2019 in una specifica area di Napoli e, tra il 2020 e il 2021, in alcuni comuni della regione Emilia-Romagna, in particolare nel territorio dell'Unione Pedemontana Parmense, un consorzio di cinque comuni in provincia di Parma[30]. L'iniziativa, sostenuta dalla Regione Emilia-Romagna, ha integrato l'uso dell'app nei gruppi di controllo di vicinato[31].

Dal punto di vista tecnico, Vigilium è concepito come un *Decision Support System* (DSS) basato su un approccio partecipativo e data-driven. I cittadini possono inviare segnalazioni anonime e non emergenziali, relative a episodi di degrado o insicurezza urbana, tramite un'applicazione mobile. Le informazioni raccolte vengono elaborate e geolocalizzate, producendo mappe del rischio, statistiche e indicatori predittivi a supporto delle decisioni delle autorità locali e delle polizie municipali[32].

La quantità di dati trattati da Vigilium è particolarmente ampia, forse la più estesa rispetto alle tecnologie analizzate finora: «dati sui crimini, dati relativi alla criminalità, all'insicurezza e al degrado urbano raccolti tramite segnalazioni anonime dei cittadini o basati su questionari inviati dalle persone attraverso un'app dedicata, dati sul disordine urbano, dati relativi alla cosiddetta "smart city", come illuminazione stradale, traffico, condizioni meteorologiche, altri dati sulle variabili socio-demografiche, e dati raccolti tramite soluzioni di videosorveglianza intelligente (quest'ultima descritta come opzionale)», nonché «dati anonimizzati dei social network e su dati mobili»[33].

5.3.5 Marvel, Protector e Precrisis

Tra i progetti più recenti di *smart urban security* sperimentati a Trento, in collaborazione con la Fondazione Bruno Kessler (FBK) e con finanziamenti dell'Unione Europea, si collocano Marvel, Protector e Precrisis, tre sistemi di intelligenza artificiale con finalità e modalità operative differenti, ma accomunati dall'essere progetti di sicurezza urbana.

Marvel (*Multimodal Extreme Scale Data Analytics for Smart City Environments*), attivo dal febbraio al dicembre 2023, si fonda su un'architettura di cal-

30 Privacy Network, *Amministrazione automatizzata*, cit.
31 ANSA, *Nel Parmense test per Vigilium, app per 'prevenire' crimini*, 30 marzo 2021.
32 Privacy Network, *Amministrazione automatizzata*, cit.
33 Ivi, p. 37.

colo distribuito che integra risorse *edge* e cloud. Il sistema raccoglie in tempo reale flussi audiovisivi da microfoni e telecamere installati sul territorio e, attraverso un approccio di *privacy by design*, li anonimizza e li elabora per alimentare modelli di IA in grado di riconoscere eventi critici e segnalarli alle forze dell'ordine. In questo senso, Marvel mira a trasformare i dati grezzi raccolti in indicatori predittivi utili al processo decisionale automatizzato per la gestione del rischio in contesti urbani.

Protector (*Protecting Places of Worship*), operativo per un breve periodo nel 2021, è invece focalizzato sulla tutela dei luoghi di culto da minacce terroristiche o da crimini d'odio. Il sistema utilizza le immagini raccolte dalle telecamere di sorveglianza cittadine – in parte le stesse impiegate da Marvel – per rilevare situazioni sospette, senza tuttavia integrare l'audio. Parallelamente, analizza i contenuti pubblicati su piattaforme come Twitter e YouTube per intercettare discorsi d'odio e sentimenti negativi, così da individuare potenziali rischi diretti a comunità religiose. Sebbene il progetto prevedesse anche una valutazione delle misure di sicurezza preesistenti e delle risposte operative delle forze dell'ordine, questa funzionalità non risulta essere mai entrata pienamente in funzione.

Infine, Precrisis (*PRotECting public spaces thRough Integrated Smarter Innovative Security*), avviato nel 2024 e tuttora in corso, è coordinato da FBK come *technical coordinator* e *work package leader*, con la partecipazione di oltre nove partner europei in sette Stati membri (Grecia, Cipro, Germania, Italia, Estonia, Bulgaria e Austria). Il progetto, della durata prevista di 24 mesi, è finalizzato a testare soluzioni integrate di protezione degli spazi pubblici, anche attraverso sistemi di sensoristica e videosorveglianza intelligente.

Nonostante le differenze funzionali, tutti e tre i sistemi sono stati sviluppati e sperimentati a Trento come parte di una strategia più ampia di "città intelligente" orientata alla sicurezza urbana. Proprio per questo, nel gennaio 2024 sono stati oggetto di attenzione da parte del Garante della Privacy, che ha riscontrato diverse criticità rispetto alla conformità al GDPR.

L'analisi condotta dal Garante per la protezione dei dati personali sui progetti Marvel e Protector (al momento della valutazione del Garante per la protezione dei dati personali, a gennaio 2024, Precrisis non trattava ancora dati personali, essendo in fase di programmazione) ha messo in evidenza una serie di violazioni significative del GDPR, con particolare riferimento al trattamento di dati sensibili[34].

In primo luogo, entrambi i sistemi hanno trattato dati personali sensibili – come quelli relativi a reati o, nel caso di Protector, potenzialmente connessi all'appartenenza religiosa – senza rispettare le tutele richieste dall'art. 9 del GDPR. Il Comune di Trento aveva giustificato tali trattamenti con un generico

[34] Si veda Privacy Network, *Amministrazione Automatizzata*, cit.

richiamo alla promozione dello sviluppo culturale, sociale ed economico, ma il Garante ha ritenuto questa base giuridica insufficiente, sottolineando che l'ente non poteva qualificarsi né come istituto di ricerca né come ufficio statistico.

Un secondo elemento critico riguarda l'assenza di adeguate salvaguardie per i diritti fondamentali. Non era stato redatto un *Data Protection Impact Assessment* (DPIA) conforme, indispensabile per progetti di videosorveglianza massiva con intelligenza artificiale. A ciò si è aggiunta una mancanza di trasparenza verso i cittadini: gli avvisi pubblici non informavano chiaramente sul fatto che i microfoni registrassero le conversazioni né sulla reale portata della condivisione dei dati con partner di progetto, Commissione Europea e soggetti terzi.

Un ulteriore problema è stato individuato nelle tecniche di anonimizzazione inefficace. Volti e targhe venivano sfocati nei video, ma non abbastanza da impedire la reidentificazione; i contenuti audio erano solo distorti, non realmente anonimizzati. Il Garante ha rilevato che si trattava, in realtà, di semplici dati pseudonimizzati, ancora pienamente soggetti al GDPR. La loro condivisione con soggetti terzi ha quindi comportato un rischio aggiuntivo per gli interessati.

Infine, è stata considerata illegittima anche la condivisione con le forze dell'ordine di dati derivanti da Twitter/X, poiché consentiva di ricostruire le reti di utenti e la tipologia di messaggi pubblicati, senza che gli utenti ne fossero consapevoli.

Nel complesso, il Garante ha ritenuto che Marvel e Protector configurassero modalità massive e invasive di sorveglianza, capaci di incidere in maniera significativa su diritti e libertà fondamentali, anche di rango costituzionale. Per queste ragioni, nel gennaio 2024 ha comminato al Comune di Trento una sanzione di 50.000 euro[35].

5.3.6 SARI

Esiste in Italia anche un sistema di riconoscimento facciale automatico degli individui in capo alle Forze di polizia, SARI (Sistema Automativo Riconoscimento Immagini). Introdotto nel 2018, è stato sviluppato dalla società italiana Reco 3.26 S.r.l. e acquistato dal Ministero dell'Interno nel 2017. La versione oggi in uso, denominata SARI Enterprise, permette alle forze di polizia di verificare l'identità di una persona mettendo a confronto il suo volto con i profili

[35] Garante per la protezione dei dati personali, Provvedimento n. 207 del 10 novembre 2022: *Linee guida sui trattamenti di dati personali per finalità di intelligenza artificiale*, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/ docweb/9977020; Privacy Network, *Amministrazione automatizzata*, cit.

conservati in un archivio dedicato. Non si tratta di uno strumento che produce prove utilizzabili in tribunale, ma di un supporto investigativo che orienta e rafforza l'attività delle indagini. I dati disponibili mostrano un utilizzo significativo del sistema: secondo un'inchiesta giornalistica, per ogni 100 reati denunciati vengono effettuate circa 60 ricerche tramite SARI, con un incremento del 65% delle interrogazioni registrate tra il 2022 e il 2023[36].

Accanto a questa versione è stato sviluppato anche un progetto parallelo, SARI Real Time, pensato per il riconoscimento facciale immediato nello spazio pubblico. Si trattava di una tecnologia potenzialmente in grado di monitorare in tempo reale i movimenti delle persone attraverso telecamere collegate al sistema. Nel 2021, tuttavia, il Garante per la protezione dei dati personali ne ha impedito l'adozione, giudicando il progetto eccessivamente invasivo: un simile impiego avrebbe comportato una forma di sorveglianza di massa continua, sproporzionata rispetto agli obiettivi dichiarati di contrasto alla criminalità e pericolosa per la tutela dei diritti fondamentali, in particolare la privacy e la libertà individuale[37].

SARI Enterprise lavora in stretta connessione con l'archivio AFIS (Automated Fingerprint Identification System), una banca dati centrale del Ministero dell'Interno che raccoglie informazioni biometriche e fotografiche. In questo sistema confluiscono non solo i dati di persone con precedenti penali, ma anche quelli di cittadini stranieri il cui status amministrativo risulti irregolare o in corso di verifica, ad esempio migranti senza documenti validi o con permesso di soggiorno scaduto, o che hanno avuto in passato un permesso di soggiorno. L'uso pratico è piuttosto semplice: a partire da una fotografia di un soggetto da identificare, SARI avvia una ricerca all'interno di AFIS e restituisce un elenco di volti ordinati in base al grado di somiglianza. Non offre quindi un'identificazione certa, ma un ventaglio di possibili corrispondenze che richiede l'intervento di un operatore per essere interpretato.

Sul piano tecnico, tuttavia, le informazioni disponibili rimangono limitate. Le autorità non diffondono dettagli sul funzionamento interno dell'algoritmo né sulla gestione dei dati, giustificando la mancanza di trasparenza con esigenze di sicurezza e di ordine pubblico.

I problemi legati a questa tecnologia sono però molti. Come si legge nel report di Privacy Network sulla giustizia automatizzata in Italia,

> Sebbene SARI Real Time non sia di fatto in uso, il dibattito sul riconoscimento facciale in tempo reale in luoghi pubblici si è nuovamente

[36] Privacy Network, *Amministrazione automatizzata*, cit.
[37] *Ibid*.

> acceso con la discussione e approvazione finale del testo dell'AI Act: la nuova normativa sull'IA sembrerebbe, ad un primo impatto, vietare quelle tecnologie in grado di porre in essere un'attività di riconoscimento biometrico real-time in luoghi pubblici, considerandolo alla stregua di un sistema che pone un rischio giudicato "inaccettabile." Tuttavia, una più approfondita analisi dello stesso art. 5 dell'AI Act, in cui sono indicate le tecnologie vietate, rivela tutt'altre intenzioni del legislatore europeo, che ha ritagliato una serie di eccezioni, anche abbastanza ampie, di utilizzo di riconoscimento biometrico real-time in luoghi pubblici. Per cui, nulla potrebbe escludere, in un futuro nemmeno troppo remoto, la riabilitazione di SARI Real Time o di strumenti simili[38].

5.3.7 I rischi della polizia predittiva in Italia

Nel paragrafo precedente abbiamo descritto i vari sistemi di controllo data-driven impiegati dalla polizia in Italia. Le informazioni non sono molte, alcune si trovano nei siti web delle compagnie proprietarie (come Xlaw), dunque non possiamo essere sicure che siano in uso tuttora. Su questo e sui dettagli del loro funzionamento bisognerebbe condurre una seria indagine empirica. Sappiamo però che sono state utilizzate. Dedichiamo allora questo ultimo breve paragrafo a individuare i rischi insiti in questi sistemi e mettere in luce eventuali differenze con i software che abbiamo analizzato in altri contesti nazionali, in Europa o negli Stati Uniti.

Innanzitutto, se dovessimo basarci sul tipo di dati utilizzati da questi sistemi, si potrebbe dire che i software in uso, o che sono stati in uso, in Italia si avvalgono in larga parte di dati prodotti dalla polizia. Questo dovrebbe metterci in parte al riparo da tutti i problemi legati all'utilizzo dei big data prodotti fuori dai contesti di polizia (violazione della privacy, *dragnet*, utilizzo per scopi di *law enforcement* di dati raccolti per scopi diversi dal *law enforcement*), ma non ci mette al riparo dal rischio che l'utilizzo di questi sistemi non riproducano dinamiche discriminatorie invece che fungere da soluzione alle stesse. Infatti, come abbiamo più volte ripetuto, i dati di polizia sono portatori di *bias*, che vengono riprodotti nel controllo algoritmico.

Tuttavia, questi sistemi non utilizzano solo dati di polizia. Abbiamo visto che alcuni raccolgono dati ambientali (trasporti, meteo, dati anagrafici, ecc.), come Xlaw, che li utilizza per costruire una città virtuale su cui poi inserire i dati di polizia, ma anche Vigilium.

Ci pone dei dubbi l'utilizzo di altre tipologie di dati come ad esempio le segnalazioni dei cittadini possibili tramite app nel caso di Vigilium. In questo caso,

[38] Privacy Network, *Amministrazione automatizzata*, cit., p. 25.

infatti, stereotipi e pregiudizi insiti in chi fa delle segnalazioni rischiano di entrare nel sistema. È un problema antico, che possiamo collegare alle analisi critiche sulla sicurezza urbana[39], che è valido tanto nell'era pre-digitale quanto in quella odierna, ovvero il problema di come le richieste di alcuni cittadini possano indirizzare le politiche di sicurezza verso alcune situazioni o alcuni soggetti percepiti come minacce, a dispetto della loro reale pericolosità[40]. Non abbiamo tempo per dilungarci qui, ma è un meccanismo che richiama quello che già Dal Lago negli anni Novanta aveva denominato «Tautologia della paura»[41]. Alcuni dubbi li solleva anche l'utilizzo delle tracce video (Precrisis) e anche audio (Marvel) dalle videocamere a circuito chiuso nel comune di Trento. Come abbiamo visto, il garante ha già valutato i rischi di violazione della privacy dovuti al fatto che l'anonimazione dei dati non sia stata ritenuta sufficiente e che le videocamere non fossero adeguatamente segnalate ai cittadini. Delicato anche l'utilizzo dei dati degli utenti estrapolati da Twitter e Youtube nel progetto Precrisis, anche questo valutato come violazione della privacy, per mancanza di consapevolezza da parte degli utenti di come i propri dati sarebbero stati utilizzati. Una particolarità del sistema Keycrime non riscontrata in altri software è l'utilizzo di dati provenienti da interviste a testimoni. Anche in questo caso, queste informazioni rischiano di essere problematiche per la loro parzialità, ma questo vale anche per le indagini senza utilizzo di tecnologia. In tutti questi casi, conoscere il funzionamento esatto dei software sarebbe importante anche per capire come ognuna di queste variabili finisce per costruire il calcolo di probabilità: che peso ha ognuna? Quale teoria criminologica è stata utilizzata per elaborare l'algoritmo? Sono interrogativi fondamentali per valutare il funzionamento di questi sistemi, sia da parte del pubblico sia da parte degli agenti che li utilizzano. Per questo sarebbe quanto più necessaria maggiore trasparenza rispetto ai dati e agli algoritmi utilizzati, possibile solo tramite una serie ricerca empirica.

Sulla questione delicata dell'opacità degli algoritmi, ciò che in letteratura abbiamo visto nominato "black box", vale la pena aprire un breve approfondimento. Infatti, in questi esperimenti di polizia predittiva, in alcuni casi la polizia stessa ha collaborato allo sviluppo dei software. Addirittura, due di essi sono stati elaborati proprio dalla polizia. È il caso di Xlaw, elaborato presso la Questura di Napoli nel 2004, prima di essere venduto a una compagnia privata, e in parte è anche il caso di Keycrime, sviluppato presso la Questura di Milano nel 2008 da Mario Venturi che poi ha fondato la propria startup. Anche Vigilium vede

---

39 O. Firouzi Tabar, *Una rassegna di ricerche sulla percezione dell'insicurezza in Italia: forza e vulnerabilità del "paradigma sicuritario"*, in *Studi sulla questione criminale*, 2014, 3, pp. 73-92.

40 R. Selmini, *Dalla sicurezza urbana al controllo del dissenso politico. Una storia del diritto amministrativo punitivo*, Roma, Carocci, 2020.

41 A. Dal Lago, *Non-persone*, Milano, Feltrinelli, 1999.

una collaborazione con la Questura di Trento in fase di elaborazione. Quattro di questi sistemi vedono invece la collaborazione dell'Università e di una fondazione privata nell'implementazione del progetto (Vigilium, Marvel, Precrisis e Protector). Nel caso di Protector, in corso di sperimentazione al momento della scrittura di questo testo, partecipano anche fondi dell'Unione Europea. Anche in Italia si vede la presenza del privato. Abbiamo infatti visto che il settore privato in alcuni casi è arrivato dopo ad acquisire un prodotto che era già stato elaborato (Xlaw acquisito da XServizi nel 2021), in altri invece è intervenuto già in fase iniziale, nell'elaborazione di un programma poi ceduto al compratore (è il caso di SARI, elaborato dalla società italiana Reco 3.26 S.r.l. e acquistato dal Ministero dell'Interno nel 2017). Insomma, anche nel caso italiano sembra importante indagare il ruolo del privato nello sviluppo – o nel non sviluppo – dei software di polizia predittiva e data-driven.

Proviamo adesso a focalizzare l'attenzione nello specifico su problemi di discriminazione che possono emergere dall'utilizzo di questi sistemi. Abbiamo già sollevato dei dubbi sulle conseguenze potenzialmente discriminatiorie delle segnalazioni da parte dei cittadini. Qui proviamo a soffermarci sui casi di discriminazione che possono provenire dall'utilizzo dei dati di polizia. Proviamo quindi a concentrarci sul caso SARI.

SARI non è un sistema di polizia predittiva, ma come abbiamo visto è un sistema di riconoscimento facciale che permette alla polizia di identificare una persona comparando l'immagine del suo volto ad altre immagini contenute nel database di polizia AFIS, con lo scopo di proporre una serie di possibili *match* tra cui poi l'operatore di polizia deve scegliere.

L'AFIS, il sistema informatizzato per la raccolta, archiviazione e confronto delle impronte digitali e di altri dati biometrici identificativi, è gestito dal Servizio Polizia Scientifica. Costituisce un archivio centrale che consente di acquisire e digitalizzare impronte raccolte durante attività di polizia o in sede forense, confrontarle automaticamente con milioni di profili già presenti, al fine di identificare persone sospette, vittime o soggetti ignoti, scambiare dati biometrici a livello internazionale. Secondo i dati riportati da IrpiMedia, nel 2022 il sistema AFIS raccoglieva complessivamente oltre 18 milioni di profili biometrici: 13.516.259 appartenenti a cittadini di Paesi extra-UE, 1.654.917 a cittadini europei e 3.289.196 a cittadini italiani[42]. Ne risulta che la quota più consistente di soggetti censiti riguarda persone straniere. L'Associazione per gli Studi Giuridici sull'Immigrazione (ASGI) ha criticato questa configurazione, definendo AFIS una banca dati discriminatoria:

[42] L. Bodrero, *Il Viminale ci tiene all'oscuro su come e quanto usa il sistema di riconoscimento facciale*, in *IrpiMedia*, 24 luglio 2024, https://irpimedia.irpi.eu/sorveglianze-viminale-riconoscimento-facciale-trasparenza.

i cittadini stranieri che ottengono successivamente la cittadinanza italiana non possono infatti chiedere la cancellazione dei propri dati se non dopo vent'anni dall'inserimento[43]. In questo modo, anche individui che non hanno commesso reati restano registrati in un archivio pensato originariamente per soggetti con precedenti penali, con il rischio di perpetuare una forma di esclusione sistemica. Questo significa che nella comparazione delle immagini di volti, SARI confronta l'immagine della persona da identificare con un archivio in cui le immagini presenti sono in grandissima maggioranza cittadini stranieri. Questo crea ovviamente dei dubbi in quanto a criteri di equo trattamento e al fatto che la sorveglianza di massa non sia poi così di massa ma piuttosto selettiva, e che riguarda soggetti già noti alle forze dell'ordine[44]. Già noti non per forza in ragione di reati che possono aver commesso, ma per chi sono (i migranti).

Dunque, anche in Italia il controllo data-driven mostra di essere una pratica sociomateriale e di doversi aprire allo scrutinio pubblico per innalzare legittimità e funzionamento.

5.4 Le pratiche sociomateriali della predizione

Da molti degli autori che si stanno occupando di studiare e raccontare i sistemi del controllo data-driven nelle forze di polizia in Europa, e che decidono di farlo adottando un'ottica critica, condividono la tesi per cui le tecnologie di *predictive policing* non siano strumenti neutri, ma dispositivi sociotecnici che incarnano specifiche visioni politiche e culturali della sicurezza. Le loro ricerche, in particolare quelle raccolte nel volume *Predictive policing in Europe. Critical perspective*[45], condividono un quadro teorico per cui la polizia predittiva non rappresenti soltanto una questione tecnica di efficienza, ma soprattutto un fenomeno politico e culturale che ridefinisce il rapporto tra polizia, cittadini e tecnologia. Questi software mostrano quanto le promesse di una polizia basata sui dati si intreccino con logiche di potere, strategie di governance e narrazioni pubbliche

[43] Asgi, *Il casellario delle identità AFIS: una banca dati discriminatoria usata dalle forze di polizia*, 9 aprile 2024, https://www.asgi.it/antidiscriminazione/casellario-afis-una-banca-dati-discriminatoria-forze-di-polizia.

[44] E. Di Molfetta, *Digital surveillance and big data policing: Local security governance in the global digital age*, presentato alla Ethnography and qualitative research international conference, 10th edition, University of Trento, 9-10 June 2025.

[45] V. Galis, H.O.I. Gundhus, A. Vradis (a cura di), *Critical Perspectives on Predictive Policing: Anticipating Proof?*, cit.

che cercano di legittimare l'uso di strumenti complessi e opachi[46]. L'uso dell'intelligenza artificiale nelle pratiche di polizia richiede un costante scrutinio critico poiché i pattern prodotti da questi sistemi e che guidano operativamente le forze dell'ordine tendono a mascherare le assunzioni, i valori e le strutture decisionali sottostanti, che rimangono spesso invisibili e non verificabili[47].

Illuminante la riflessione a questo proposito di Meijer e Wessels, secondo cui la predizione algoritmica nel contesto della polizia predittiva non è mai solo un fatto tecnico, ma si fonda su "pratiche sociomateriali" (*sociomaterial practices*). Questa espressione fa riferimento all'intreccio di pratiche sociali (decisioni politiche, priorità istituzionali, visioni culturali della sicurezza) e materiali (dati raccolti, infrastrutture tecnologiche, modelli statistici) che insieme danno forma ai processi predittivi. In altre parole, gli algoritmi non "parlano da soli": il modo in cui sono costruiti e impiegati riflette scelte sociali, valori e contesti specifici. Ad esempio, se i dati usati per l'addestramento provengono da aree storicamente più sorvegliate, il risultato sarà un rafforzamento dei *bias* preesistenti. La "materialità" delle pratiche si vede nel codice, nei database e nei sistemi tecnici; la dimensione "sociale" si manifesta nelle decisioni su come questi strumenti vengono applicati, interpretati e giustificati. Meijer e Wessels collegano questa idea al fatto che le correlazioni trovate dagli algoritmi rischiano di essere prese come verità oggettive, ma in realtà derivano da un contesto socio-materiale che condiziona sia ciò che viene predetto sia il modo in cui le previsioni vengono usate. In questo senso, le «sociomaterial practices underpinning prediction» mostrano che non possiamo separare la tecnica (gli algoritmi) dalla società che li produce e li utilizza[48].

Facciamo alcuni esempi per rendere più concreta questa idea di pratiche sociomateriali che sostengono la predizione: ciò che viene considerato "dato rilevante" dipende da scelte organizzative e politiche. Ad esempio, includere o escludere certi reati dai database non è un'operazione neutra: influenza direttamente le previsioni; nei sistemi di *predictive mapping* (che segnalano zone a rischio), l'algoritmo produce mappe di "hotspots", ma è la polizia a decidere come e quanto pattugliare quelle aree. La predizione tecnica, dunque, si intreccia con le pratiche sociali della polizia e con le percezioni pubbliche di sicurezza; anche quando un algoritmo segnala un rischio elevato, il modo in cui le autorità interpretano quella previsione dipende da norme giuridiche, priorità istituzionali o pressioni politiche. Ad esempio, un comune può scegliere di destinare più ri-

[46] Karlsson, V. Galis, *POL-INTEL: Predictive policing and the politics of data integration in Denmark*, cit.

[47] M. Kaufmann, *AI in policing and law enforcement*, cit.

[48] A. Meijer, M. Wessels, *Predictive Policing: Review of Benefits and Drawbacks*, cit.

sorse a pattugliamenti visibili per rassicurare i cittadini, piuttosto che a indagini mirate. Questi esempi mostrano che la predizione non nasce solo dal "calcolo" algoritmico, ma da un'ibridazione costante tra tecnologia e società: database, software e modelli matematici sono "materiali", ma sono plasmati da pratiche sociali che ne orientano la forma e l'uso.

Meijer e Wessels[49] adottano una prospettiva più tecno-ottimista che tecno-pessimista sulla polizia predittiva: invece di considerarlo uno strumento inevitabilmente distopico o intrinsecamente discriminatorio, lo analizzano per l'appunto come un insieme di pratiche socio-materiali, in cui dati, algoritmi e infrastrutture tecnologiche si intrecciano con decisioni politiche, priorità organizzative e contesti sociali. Questa impostazione consente loro di mettere in luce aspetti che spesso sfuggono alle analisi più critiche. In primo luogo, la loro lettura multilivello, che considera la predizione come il prodotto di processi diversi (raccolta dati, costruzione degli algoritmi, implementazione operativa, effetti sociali), sottolinea come molte criticità emergano non tanto dall'algoritmo in sé, quanto dal modo in cui i risultati vengono interpretati e utilizzati. Se esiste un problema di discriminazione e di selettività del controllo, questa va ricercata non tanto – o non unicamente – nell'utilizzo delle tecnologie data-driven ma è un problema antico come la polizia e ha a che fare con la sua cultura, il suo potere discrezionale e il suo mandato: mantenere l'ordine e, al contempo, prendere delle decisioni su cosa sia ordine e cosa no[50]. In secondo luogo, riconoscono che la polizia predittiva potrebbe generare anche benefici potenziali, come una maggiore efficienza organizzativa o una gestione più mirata delle risorse, andando oltre la mera logica repressiva che spesso domina il dibattito. Infine, introducono un aspetto innovativo rispetto ad altri autori: il tema della legittimità. Per loro, infatti, non è sufficiente che un sistema predittivo sia tecnicamente accurato: la sua accettabilità sociale e politica dipende dalla possibilità per i cittadini e gli elettori di comprendere, valutare e controllare le scelte incorporate negli algoritmi. Ciò implica la necessità di maggiore trasparenza procedurale, audit indipendenti e strumenti di contestazione pubblica, che mancano ancora, ma senza i quali la fiducia nella polizia rischia di deteriorarsi.

---

[49] *Ibid*.

[50] G. Fabini, E. Gargiulo, D. Tuzza, *Polizia: un vocabolario dell'ordine*, cit.

6. Conclusioni. La sicurezza dei dati e la sicurezza dai dati

Tradizionalmente, la cybersicurezza è stata associata al settore privato, agli esperti informatici e alle agenzie governative specializzate[1]. Tuttavia, la polizia ricopre un ruolo altrettanto decisivo nel fronteggiare le minacce informatiche che colpiscono cittadini e società nel loro complesso. La sua azione si articola su più livelli. Da un lato vi è la dimensione investigativa: la polizia è chiamata a identificare gli autori di reati informatici – *hacking*, frodi online, furti di dati, distribuzione di *malware*, attacchi alle infrastrutture critiche – ricorrendo a tecniche avanzate di analisi digitale e a strumenti di informatica forense per raccogliere prove elettroniche e rintracciare i responsabili. Dall'altro lato vi è la dimensione preventiva: le forze dell'ordine operano per proteggere infrastrutture strategiche come reti di comunicazione, banche, istituzioni pubbliche e servizi governativi, riducendo la probabilità e l'impatto di eventuali attacchi. A ciò si aggiungono attività di sensibilizzazione dei cittadini sui rischi connessi alla vita online, condotte spesso in collaborazione con scuole, comunità locali o associazioni, e partnership operative con esperti di sicurezza e attori privati per innalzare i livelli complessivi di protezione. Quando si verificano violazioni o attacchi, infine, la polizia partecipa alla gestione degli incidenti, coordinando interventi rapidi per contenere i danni, identificare i responsabili e ripristinare la fiducia dei cittadini.

L'intersezione fra big data e cybersicurezza rende tuttavia ancora più complesso questo quadro. Da un lato, l'uso massiccio di dati apre nuove opportunità investigative: le tecniche di data-driven consentono di elaborare previsioni e di

[1] R. Brighi, *Introduzione al concetto di cybersicurezza: una prospettiva informatico-giuridica*, in *Governare la sicurezza degli (eco)sistemi cyberfisici. Regolamentazione, diritti e politiche*, Torino, Giappichelli, 2025.

orientare le risorse verso aree o comportamenti a rischio, mentre l'analisi dei grandi insiemi informativi provenienti da partnership con aziende private, strumenti di sorveglianza o fonti aperte permette di ampliare la capacità di monitoraggio. Dall'altro, proprio la natura e la mole di questi dataset sollevano rischi considerevoli. In primo luogo, la provenienza dei dati deve essere trasparente: se i cittadini non comprendono come vengano raccolti, condivisi o utilizzati, la fiducia nelle istituzioni rischia di erodersi. In secondo luogo, la sicurezza di archivi così vasti rappresenta una sfida cruciale[2]: una violazione non comprometterebbe soltanto la privacy individuale, ma potrebbe danneggiare intere comunità, esporre informazioni sensibili e minare la credibilità stessa delle forze dell'ordine. Inoltre, è l'uso stesso che si fa dei big data che, anche senza nessun rischio di furto dei dati, può essere fonte di danno sociale per soggetti singoli e per intere comunità[3]. In questo senso, i big data sono al tempo stesso risorsa strategica e potenziale vulnerabilità critica.

In queste riflessioni conclusive proviamo allora a parlare da un lato di polizia e sicurezza *dei* big data, ossia le modalità con cui tali informazioni devono essere protette; dall'altro di polizia e sicurezza *dai* big data, vale a dire le implicazioni e i rischi che l'uso massiccio dei dati comporta per i diritti e le libertà dei cittadini.

Sicurezza dei dati. Gli episodi di data *breach* dei database di polizia non sono così rari. Protagonista di uno di questi episodi è la Police Service of Northern Ireland (PSNI), in Irlanda del Nord. L'8 agosto 2023, nel corso di una risposta a una richiesta di accesso civico (FOI), la PSNI ha pubblicato online un file di calcolo che conteneva, in una scheda "nascosta", i dati personali dell'intera forza lavoro (9.483 persone): cognome, iniziale del nome, grado/ruolo e sede/unità. Si è trattato di un errore procedurale nella gestione e pubblicazione di un foglio elettronico a valle di FOI. L'Information Commissioner's Office ha poi annunciato un'ammenda di £750.000 e ha descritto le carenze procedurali rilevate. Anche la polizia olandese è stata protagonista di un episodio di *datalek* che ha riguardato i dati personali dei lavoratori (contatti di servizio) contenuti nelle directory interne della polizia. Il 26 settembre 2024, il Ministero della Giustizia e Sicurezza dei Paesi Bassi ha informato il Parlamento di un *datalek* che ha portato all'esfiltrazione di dati di contatto "work-related" di tutti i dipendenti della polizia (nomi, funzioni, indirizzi email istituzionali, numeri di servizio). La Polizia

[2] M. Kusak, *Quality of data sets that feed AI and big data applications for law enforcement*, in *ERA Forum*, 2022, 23(2), pp. 209-219.

[3] R. Van Brakel, L. Govaerts, *Exploring the impact of algorithmic policing on social justice: Developing a framework for rhizomatic harm in the pre-crime society*, in *Theoretical Criminology*, 2024, 29(1), pp. 91-109.

nazionale successivamente ha chiarito che si trattava di informazioni presenti nei "biglietti da visita" digitali e, in alcuni casi, immagini associate.

Le due forze di polizia, Norfolk e Suffolk Police, in Inghilterra, hanno invece diffuso per errore i dati relativi alle vittime e ai sospetti di reati. Sempre ad agosto 2023, le Norfolk e Suffolk Police hanno reso noto che, a causa di un problema tecnico, in alcune risposte FOI (aprile 2021-marzo 2022) sono stati inclusi – all'interno dei file rilasciati – dati provenienti dal sistema di gestione dei reati: informazioni identificative su vittime, testimoni e sospetti e descrizioni degli illeciti (domestici, reati sessuali, aggressioni, furti, *hate crime*). Le due forze di polizia hanno dato comunicazione del numero degli interessati (1.230) e dell'invio delle notifiche.

Un trapelamento di dati personali ha riguardato, al luglio 2022, i dati custoditi dalla polizia di Shanghai, in Cina. A quanto pare, un soggetto ha offerto in vendita in un forum di hacking circa 23 TB di dati che sosteneva provenissero dalla banca dati della polizia di Shanghai e che riguardassero fino a 1 miliardo di cittadini. Si trattava di informazioni personali e relativi a casi. L'episodio, se confermato nella sua interezza, rappresenta uno dei *leak* più vasti mai segnalati.

In India, è stato individuato a maggio 2024 un server esposto (quasi 500 GB per 1,6 milioni di documenti), collegato alla società *ThoughtGreen Technologies* (*outsourcing IT*), contenente dati biometrici e personali relativi a membri delle forze dell'ordine e candidati alla polizia, nonché ad altri civili come insegnanti, personale ferroviario. I dati includevano impronte digitali, immagini facciali, firme, dettagli di tatuaggi e cicatrici, oltre a certificati e documenti identificativi[4] ed erano conservati in un web storage aziendale non protetto appartenente a un fornitore terzo.

Anche in Italia pare si siano verificati degli episodi di accesso illecito ai dati di cittadini UE. Le accuse – attualmente oggetto di verifica da parte delle autorità competenti – sono state portate a galla da un'inchiesta giornalistica. Secondo tale inchiesta, un reparto di polizia italiano avrebbe consultato illecitamente dati anagrafici di conducenti UE dai registri veicolari nazionali e li avrebbe condivisi con Euro Parking Collections, una società che gestisce per conto di Transport for London sanzioni LEZ/ULEZ. Altri riscontri giornalistici hanno riportato che autorità olandesi (RDW) e tedesche (KBA) hanno segnalato l'uso

[4] C. Krol, *Police biometrics exposed in India data breach*, in *Wired*, 23 maggio 2024, https://www.wired.com/story/police-face-recognition-biometrics-leak-india; J. Fowler, *Data breach exposes biometric and personal information in India*, in *WebsitePlanet Research*, 23 maggio 2024, https://www.websiteplanet.com/news/police-biometric-data-breach-india.

improprio di canali di cooperazione (National Contact Point) pensati per reati stradali di sicurezza, non per violazioni ambientali[5].

La protezione delle banche dati gestite dalla polizia – contenenti informazioni sensibili su milioni di individui – costituisce una questione cruciale. Questi esempi di cronaca parlano di uno dei due aspetti nel rapporto tra polizia, cybersecurity e big data: la sicurezza dei dati che la polizia acquisisce, produce, conserva e utilizza per le attività di controllo, prevenzione e indagine. Oggi, parlare di cybersecurity in connessione alla polizia significa anche parlare di questo. Infatti, l'adozione crescente delle tecnologie di big data nelle attività di polizia ha introdotto sfide significative in materia di protezione dei dati. Il successo delle applicazioni data-driven dipende dalla protezione di vasti dataset che comprendono informazioni personali e non personali sensibili. In assenza di controlli e misure adeguate, i dati sensibili raccolti durante le indagini possono essere vulnerabili a furti o perdite, compromettendo sia le prove digitali sia i dati personali dei cittadini coinvolti. Inoltre, la mancanza di risorse e di formazione adeguata nel personale di polizia accresce le vulnerabilità, aumentando il rischio di incidenti informatici. La crescente dipendenza delle forze dell'ordine da sistemi di archiviazione su cloud e da strumenti di analisi in tempo reale incrementa ulteriormente l'esposizione a incidenti informatici. Sistemi interoperabili centralizzano enormi quantità di dati personali – come profili biometrici, informazioni genetiche e tracce provenienti dai social media – rendendoli particolarmente vulnerabili. L'uso di piattaforme come Palantir, che integrano dati eterogenei provenienti da social media, sistemi di sorveglianza e registri giudiziari, rende cruciale la garanzia di sicurezza e integrità. Diversi studi hanno inoltre messo in evidenza i rischi specifici associati ai big data in polizia. Da un lato, le tecnologie amplificano le probabilità di violazioni e fughe di dati, con conseguenze potenzialmente catastrofiche per indagini e fiducia pubblica[6], soprattutto quando grandi database sono interconnessi tra diverse giurisdizioni[7]. Dall'altro, l'infrastruttura digitale stessa delle forze dell'ordine diventa un bersaglio sempre più esposto a *ransomware*, hacking e manipolazione dei dati da parte di attori ostili intenzionati a sfruttarne le vulnerabilità[8]. Alle minacce esterne appena descritte

---

5 P. Greenfield, *Italian police accused of illegally accessing EU drivers' data to enforce London Ulez fines*, in *The Guardian*, 8 febbraio 2024, https://www.theguardian.com/environment/2024/feb/08/ulez-fines-scandal-italian-police-illegally-accessed-thousands-of-eu-drivers-data.

6 A. Babuta, *Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities*, London, Royal United Services Institute (RUSI), 2017.

7 P. Fussey, S. Roth, *Digitizing the Governance of Security Infrastructure: Big Data, Predictive Analytics and Surveillance*, in *Surveillance & Society*, 2020, 18(2), pp. 204-221.

8 S. Brayne, *Big Data Surveillance: The Case of Policing*, cit. Intorno al tema della cybersicurezza si è mossa una forte produzione normativa a livello europeo negli ultimi anni. Sin dal 2013, l'approccio pro-

si aggiungono i rischi interni: senza controlli stringenti, protocolli di accesso chiari e formazione adeguata, i dati sensibili possono essere abusati per fini illeciti, sia per errore umano sia per condotte intenzionali. Non mancano, infatti, casi documentati di accessi impropri da parte del personale di polizia, che hanno compromesso indagini e alimentato la sfiducia dei cittadini[9].

Sicurezza dai dati. La cybersicurezza, quando viene applicata all'uso dei big data nelle pratiche di polizia, non può essere ridotta a un insieme di accorgimenti tecnici. Essa deve essere concepita come parte integrante di un quadro giuridico e sociale più ampio[10], capace di bilanciare l'efficienza investigativa e la protezione dei dati personali con la tutela dei diritti fondamentali, mentre cerca di identificare e correggere le storture e le cattive pratiche che possono derivare da un uso fallace dei big data. Da una prospettiva critica e criminologica, è quindi essenziale interrogarsi sui rischi delle tecnologie di controllo in termini di sovraccarico di sorveglianza, violazioni della privacy, distorsioni algoritmiche e discriminazioni potenziali. Le misure di protezione dei dati non sono soltanto strumenti tecnologici, ma anche dispositivi normativi e garanzie democratiche, indispensabili per evitare derive verso pratiche di sorveglianza eccessiva o discriminatoria.

In questa prospettiva, l'analisi delle relazioni tra uso dei big data nelle pratiche di polizia e cybersicurezza non si limita a descrivere strumenti e metodologie, ma affronta le vulnerabilità insite nel ricorso a tecnologie di controllo basate sui dati. Affrontare in modo proattivo i *bias* e le criticità connesse all'uso dei big data e degli algoritmi significa comprendere come tali strumenti possano, se non adeguatamente regolati, rafforzare disuguaglianze sociali ed espandere la cultura della sorveglianza. Quindi, corretto uso dei dati e protezione degli utilizzatori finali significa anche controllare come questi dati vengono utilizzati, che effetti producono.

---

mosso è di tipo globale, basato sulla cooperazione internazionale, la condivisione di informazioni e la redistribuzione di responsabilità tra settore pubblico e privato in tre macroaree: la resilienza, il contrasto al cybercrimine, la cyberdifesa e la cyberdiplomazia. In tale ottica, è stato rafforzato il ruolo dell'ENISA (Agenzia dell'Unione Europea per la cybersicurezza), mentre in Italia è stata creata l'ACN (Agenzia per la Cybersicurezza Nazionale). Vedi R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano: Franco Angeli 2023; R. Brighi e P.G. Chiara, L*a cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, cit.; M. Buffa, *La direttiva NIS II. Cybersecurity in Europa: tra innovazione, formazione e diritto vivente,* in *Democrazia E Diritti Sociali*, 2023, 1, pp. 47-64. Anche le infrastrutture digitali della polizia devono rispettare queste norme.

9 R. Van Brakel, A. Meijer, *Predictive Policing: The Role of Big Data in Policing*, in *Information Polity*, 2018, 23(3), pp. 222-234.

10 Per un'idea di sicurezza come funzione pubblica si vedano: T.F. Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni Costituzionali*, 2024(2); R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano: Franco Angeli 2023.

È essenziale che le informazioni immesse nei sistemi di big data siano accurate, affidabili e aggiornate. Errori nella raccolta o nell'elaborazione possono generare falsi positivi, individuazioni errate o analisi viziate, soprattutto quando nei dataset si annidano pregiudizi storici. I sistemi predittivi mostrano come dati incompleti o inaccurati possano perpetuare *bias* e disuguaglianze nelle pratiche di polizia[11]. La mancanza di misure adeguate di cybersicurezza può inoltre consentire a soggetti ostili di manipolare o corrompere i dati, producendo analisi distorte e decisioni ingiuste. Le implicazioni etiche dell'uso improprio si intrecciano così ai rischi interni, rafforzando la necessità di sistemi rigorosi di tracciabilità delle operazioni, controlli degli accessi e meccanismi di *accountability*[12].

Questo mutamento nell'approccio alla cybersecurity nelle società digitali impone un'interpretazione più ampia anche di che cosa si debba intendere con *cyber incident.* Forse, se letto nel contesto di una società digitale, riconoscendo quindi che la cybersecurity riguarda intrinsecamente la tutela della sicurezza individuale e collettiva in una realtà complessa e ibrida, il *cyber incident* dovrebbe includere un ventaglio più esteso di rischi rispetto a violazioni strettamente tecniche, come furto di dati o intrusione nei sistemi[13]. Infatti, una violazione di dati, che può inizialmente apparire come un evento puramente tecnico, mostra di determinare conseguenze più ampie – quali l'uso improprio delle informazioni personali o l'erosione della fiducia pubblica – rivelano la sua profonda portata a livello sociale[14].

---

11 R. Richardson, J. M. Schultz, K. Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, in *NYU Law Review Online*, 2019, 94, pp. 192-233.

12 S. Brayne, *Big Data Surveillance: The Case of Policing*, cit.

13 Risuonano in questo senso alcune interessanti riflessioni di Piergiorgio Chiara in merito a un diritto soggettivo alla cybersecurity. Chiara sottolinea che non tutti i cyberincidenti comportano una violazione di dati personali, ma ciò non significa che siano privi di impatto per gli individui. Un attacco informatico può infatti causare danni materiali, psicologici o sociali anche in assenza di accesso o compromissione di dati personali. È il caso, ad esempio, di un ransomware che blocca l'accesso a un dispositivo o a un servizio essenziale, oppure di un attacco a un sistema IoT domestico che altera il funzionamento di dispositivi connessi. Poiché il GDPR tutela solo i casi in cui vi sia un pregiudizio per i dati personali, questi scenari restano giuridicamente scoperti. Per questo motivo, Chiara sostiene la necessità di riconoscere un diritto fondamentale alla cybersecurity, capace di garantire protezione anche in presenza di minacce digitali che non rientrano nella definizione di data breach, ma che compromettono comunque la sicurezza e l'integrità della vita digitale degli individui. P.G. Chiara, *Towards a right to cybersecurity in EU law? The challenges ahead*, in *Computer Law & Security Review*, 53, 105961.

14 T.F. Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni Costituzionali*, 2024(2); R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano: Franco Angeli 2023; M. Pietrangelo, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista Italiana di Informatica e Diritto*, 2024(2), pp. 13-24; R. Brighi, *Introduzione al concetto di cybersicurezza: una prospettiva*

Queste conseguenze possono essere comprese alla luce di ciò che Floridi[15] definisce "danno informazionale" – vale a dire un danno che non deriva da violenza fisica o coercizione esplicita, bensì dall'uso improprio, dalla distorsione o dall'applicazione ingiusta delle informazioni. Il danno informazionale incide sulla dignità, sull'autonomia e sull'identità sociale delle persone, e si manifesta spesso sotto forma di trattamenti discriminatori, danni reputazionali o forme di esclusione.

Se proviamo a ragionare di polizia predittiva in termini di *cyber incident*, l'impiego distorto di strumenti predittivi potrebbe essere considerato un incidente informatico. È infatti importante riconoscere che il danno digitale può anche prodursi attraverso il funzionamento routinario di sistemi difettosi, ovvero che presentano errori strutturali, difetti di progettazione o funzionamento, cioè carenze tecniche o concettuali che ne compromettono l'affidabilità. Il danno digitale può prodursi anche attraverso il funzionamento routinario di sistemi faziosi, che incorporano *bias*, ossia distorsioni o pregiudizi che, come abbiamo visto nel secondo capitolo, spesso derivano dai dati con cui sono stati addestrati o dalle logiche con cui sono stati progettati e che producono risultati sistematicamente squilibrati o discriminatori (per genere, etnia, status socioeconomico, ecc.). In questa lettura espansiva di cybersicurezza e incidente informatico, l'utilizzo di tecnologie di polizia predittiva che si basano su algoritmi discriminatori o big data gravati da *bias* costituisce una forma di vulnerabilità sistematica con conseguenze tangibili.

Qui risulta utile richiamare le critiche di Daniel J. Solove, uno dei principali studiosi di *privacy law*, alle concezioni giuridiche tradizionali di danno, che vedono il danno come risultato di lesioni dirette e visibili[16]. Solove sostiene che le violazioni della privacy implicano spesso effetti cumulativi (si accumulano nel tempo) e sistemici (non legati a un singolo atto) – quali l'esclusione, il *profiling* o il danno reputazionale – che derivano dalle modalità con cui i dati vengono raccolti, analizzati e utilizzati nel tempo. Dunque, la violazione dei dati personali è fonte di danno, anche in assenza di violazioni tecniche o intenzionalità malevola. Per questo, risultano difficili da dimostrare con i criteri giuridici tradizionali. Processi ordinari come la raccolta, l'elaborazione e la diffusione dei dati, possono produrre danni anche in assenza di intenti malevoli[17]. Da questa concezione

---

informatico-giuridica in Governare la sicurezza degli (eco)sistemi cyberfisici. Regolamentazione, diritti e politiche, Giappichelli 2025.

15 L. Floridi, *The Ethics of Information*, Oxford, Oxford University Press, 2013.

16 D.J. Solove, *Understanding Privacy*, Cambridge (MA), Harvard University Press, 2008.

17 D.J. Solove, *A taxonomy of privacy*, in *University of Pennsylvania Law Review*, 2006, 154(3), pp. 477-560.

del danno informazionale di Solove non si fa fatica a tracciare un parallelo con il dibattito intorno al concetto di danno sociale radicato nella disciplina della criminologia critica e sviluppatosi in un nuovo filone di studi, la zemiologia[18]. Il senso di parlare di danno invece che di crimine, per la criminologia critica, risiede nel fatto che esistono molti atti che, seppur non codificati come violazioni del diritto penale, sono in grado di infliggere seri danni agli individui e alle comunità, anche più della criminalità. Poter parlare di danno invece che di criminalità consente di inserire l'analisi sulla sicurezza all'interno di un ragionamento molto più ampio, che non include solo la criminalità, ma anche tutti quei comportamenti dannosi per la società (la precarietà lavorativa, lo sfruttamento, i processi di gentrificazione, l'edificazione incontrollata, il sessismo a ogni suo livello, il razzismo a ogni suo livello, ecc.) non codificati come reati. Inoltre, consente di individuare dei danni anche nei meccanismi di controllo messi in atto per governare la criminalità: il riferimento va ai danni sociali della carcerazione, a quelli legati al controllo delle migrazioni e dei confini, o anche ai processi.

Tornando a Solove[19], egli identifica varie modalità con cui il trattamento dei dati personali può violare la privacy. Alcune categorie sono particolarmente rilevanti per questo discorso: *Information processing* (es. *profiling*, identificazione, esclusione): anche un uso legale e autorizzato dei dati può produrre effetti discriminatori o dannosi; *Information dissemination* (es. *exposure*, *appropriation*): la circolazione eccessiva o decontestualizzata dell'informazione può danneggiare la reputazione o l'autonomia; *Invasion*: anche senza diffusione o raccolta eccessiva, certe pratiche possono ledere la libertà individuale (es. sorveglianza costante). E allora, il pensiero di Solove legittima l'idea che ci siano "incidenti" digitali anche in assenza di attacco. Ad esempio, se un sistema di *predictive policing* opera in modo discriminatorio per via dei dati o degli algoritmi, si verifica un danno sociale e personale reale, anche se nessuna legge sulla sicurezza informatica è stata violata. Nel caso della polizia predittiva, l'architettura informazionale stessa può generare esiti diseguali e ingiusti, in particolare a svantaggio delle comunità marginalizzate, anche in assenza di un intento malevolo.

Nel tentativo di delineare un'alternativa eticamente sostenibile all'uso opaco e unilaterale dei dati nella polizia predittiva, Ferguson introduce il concetto di *bright data*, ovvero dati utilizzati in modo trasparente, responsabile e orientato al bene pubblico. A differenza dei *black data*, che sono spesso invisibili, incontestabili e legati a pratiche discriminatorie, e dei *blue data*, che documentano l'operato

[18] V. Canning, S. Tombs, *From Social Harm to Zemiology: A Critical Introduction*, London-New York, Routledge, 2021.

[19] D. J. Solove, *A taxonomy of privacy*, cit.

della polizia ma raramente sono messi a disposizione per finalità di accountability, i *bright data* rappresentano una possibilità di riscatto tecnologico. Si tratta, secondo Ferguson, di dati che non servono a sorvegliare, classificare o criminalizzare, ma piuttosto a comprendere, prevenire e correggere fenomeni di marginalità e insicurezza. Questi dati sono accessibili, contestabili, e integrabili nei processi decisionali pubblici. Ferguson propone alcuni esempi concreti di utilizzo virtuoso del *bright data*. Uno è il progetto HunchLab, una piattaforma di analisi predittiva che, oltre a individuare le zone a rischio, include indicatori "etici" nel suo algoritmo: ad esempio, limita gli interventi della polizia in prossimità di scuole o luoghi sensibili, per ridurre il rischio di effetti collaterali sulla popolazione più vulnerabile. Un altro esempio riguarda l'uso di dati per orientare politiche di prevenzione sociale, come interventi mirati di assistenza sociale o educativa nei confronti di soggetti considerati a rischio di devianza, non per punirli, ma per offrire loro supporto prima che si verifichino comportamenti problematici. In questo senso, i *bright data* sono associata a un cambio di paradigma: non più solo previsione del crimine, ma comprensione delle cause strutturali che lo generano.

Ferguson propone così una visione del *data-driven policing* che non sia intrinsecamente repressiva, ma che possa diventare uno strumento di giustizia e trasparenza, se orientato in modo deliberato verso obiettivi di equità e responsabilità istituzionale. I *bright data* non sono solo una categoria tecnica, ma una possibilità politica e culturale: quella di recuperare la dimensione umana e collettiva della sicurezza, mettendo la tecnologia al servizio della democrazia [20].

La criminologia critica può e dovrebbe offrire un contributo alla costruzione di *bright data*. Assumendo un atteggiamento non tecnopessimista, ma attento e critico, la tecnologia data-driven potrebbe essere utilizzata in senso virtuoso, per risignificare la sicurezza dei dati come anche sicurezza dai dati e contribuire alla costruzione di un percorso comune, collettivo, pubblico e trasparente, in cui la tecnologia possa essere disegnata sulla base non delle teorie criminologiche classiche che adesso nutrono gli algoritmi di analisi, quelle basate su prevenzione situazionale e criminalità seriale, ma teorie ampie, che vedono nella struttura sociale le radici della criminalità e contribuiscano a ripensare al controllo in termini di sicurezza sociale.

[20] G. Ferguson, *The rise of big data policing*, cit., pp. 146-149.

Bibliografia

Anderson, C., *The end of theory: The data deluge makes the scientific method obsolete*, in *Wired Magazine*, 23 giugno 2008

Andrejevic, M., *Ubiquitous surveillance*, in K. Ball, K. Haggerty, D. Lyon (a cura di), *The Routledge Handbook of Surveillance Studies*, Abingdon-Oxon, Routledge, 2012, pp. 91-98.

Aragona B., Stefanizzi S., *Società digitale: interrogativi, aree di ricerca e ruolo della sociologia*, in *Sociologia Italiana*, 2024, 7, pp. 7-19.

Asgi, *Il casellario delle identità AFIS: una banca dati discriminatoria usata dalle forze di polizia*, 9 aprile 2024. https://www.asgi.it/antidiscriminazione/casellario-afis-una-banca-dati-discriminatoria-forze-di-polizia/

Association of Chief Police Officers of England, Wales and Northern Ireland (ACPO), *E-crime Strategy*, London, ACPO, 2009.

Austin, J. L., *How to Do Things with Words*, Cambridge (MA), Harvard University Press, 1975.

Babuta, A., *Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities*, London, Royal United Services Institute (RUSI), 2017.

Bauman, Z., *Liquid Modernity*, Cambridge, Polity, 2000.

Bennett Moses, L., Chan, J., *Algorithmic prediction in policing: Assumptions, evaluation, and accountability*, in *Policing and Society*, 2018, 28(7), pp. 806-822.

Berk, R., *Criminal Justice Forecasts of Risk: A Machine Learning Approach*, New York, Springer, 2012.

Bittner, E., *The Functions of the Police in Modern Society: A Review of Background Factors, Current Practices, and Possible Role Models*, Washington (DC), National Institute of Mental Health, Center for Studies of Crime and Delinquency, 1970,

Bittner, E., *The police on Skid-Row: A Study of Peace Keeping*, in *American Sociological Review*, 1967, 32(5), pp. 699-715.

Bizzini, M., *The Rise and Fall of a Predictive Policing Pioneer*, AlgorithmWatch, 2024. https://algorithmwatch.org/en/predictive-policing-pioneer-keycrime.

Bodrero, L., *Il Viminale ci tiene all'oscuro su come e quanto usa il sistema di riconoscimento facciale*, IrpiMedia, 24 luglio 2024. https://irpimedia.irpi.eu/sorveglianze-viminale-riconoscimento-facciale-trasparenza/

Borah, P., *Conceptual issues in framing theory: A systematic examination of a decade's literature*, in *Journal of Communication*, 2011, 61(2), pp. 246-263.

Bosworth, M., Hoyle, C. (a cura di), *What is criminology?*, Oxford, Oxford University Press, 2011.

Bourdieu, P., *The forms of capital*, in J.G. Richardson (a cura di), *Handbook of Theory and Research for the Sociology of Education*, Westport, Greenwood Press, 1986, pp. 241-258.

Bowling, B., Reiner, R., Sheptycki, J.W.E., *The Politics of the Police* (5ª ed.), Oxford, Oxford University Press, 2019, pp. 31-32.

boyd, d., Crawford, K., *Critical questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon*, in *Information, Communication & Society*, 2012, 15(5), pp. 662-679.

Brakel, R. V., *Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing*, in B. van der Sloot, D. Broeders, E. Schrijvers (a cura di), *Exploring the Boundaries of Big Data*, Amsterdam, Amsterdam University Press, 2016.

Brannigan, S., *High-tech crimes revealed: Cyberwar stories from the digital front*, New York, NY, Addison-Wesley, 2005

Brar, H.S., Kumar, G., *Cybercrimes: A Proposed Taxonomy and Challenges*, in *Journal of Computer Networks and Communications*, 2018, pp. 1-18

Brayne, S., *Predict and Surveil. Data, discretion and the future of policing*, New York, New York University Press, 2021.

Brayne, S., *Big Data Surveillance: The Case of Policing*, in *American Sociological Review*, 2017, 8,1, pp. 977-1008.

Brighi R., *Introduzione al concetto di cybersicurezza: una prospettiva informatico-giuridica* in *Governare la sicurezza degli (eco)sistemi cyberfisici. Regolamentazione, diritti e politiche*, Torino, Giappichelli, 2025.

Brighi, R., *Il ruolo dei dati informatici nella costruzione della realtà. Tra vulnerabilità e esigenze di trasparenza*, Roma, Aracne, 2016.

Brighi, R., Chiara, P.G., *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi*, 2021, 21, pp. 18-42.

Bryant, R. (a cura di), *Investigating digital crime*, London, Wiley-Blackwell, 2008.

Buffa, M., *La direttiva NIS II. Cybersecurity in Europa: tra innovazione, formazione e diritto vivente*, in *Democrazia e Diritti Sociali*, 2023, 1, pp. 47-64.

Butler, J., *Gender Trouble: Feminism and the Subversion of Identity*, New York-London, Routledge, 1990.

Caliskan, A., Bryson, J.J., Narayanan, A., *Semantics derived automatically from language corpora contain human-like biases*, in *Science*, 2017, 356(6334), pp. 183-186.

Campesi, G., *Genealogia della pubblica sicurezza: teoria e storia del moderno dispositivo poliziesco*, Verona, Ombre corte, 2009.

Canning, V., Tombs, S., *From Social Harm to Zemiology: A Critical Introduction*, London-New York, Routledge, 2021.

Carter, D.L., *Computer crime categories: How techno-criminals operate*, in *FBI Law Enforcement Bulletin*, 1995, 7, pp. 21-27.

Castigli, M., *L'Italia fa già "polizia predittiva" ed è ad "alto rischio" ma non vietata dall'UE: ecco perché*, Cybersecurity360, 19 giugno 2023. https://www.cybersecurity360.it/news/litalia-fa-gia-polizia-predittiva-e-ad-alto-rischio-ma-non-vietata-dallue-ecco-perche/

Chan, J., Bennett Moses, L., *Is Big Data challenging criminology?*, in *Theoretical Criminology*, 2016, 20(1), pp. 21-39.

Chan, J., Bennett Moses, L., *Using Big Data for legal and law enforcement decisions: testing the new tools*, in *UNSW Law Journal*, 2014, 37(2), pp. 643-678.

Chiara, P.G., *Towards a right to cybersecurity in EU law? The challenges ahead*, in *Computer Law & Security Review*, 2024, 53, 105961.

Cinelli, V., *Crime prevention and predictive analysis: the Italian case*, Agenfor Media, 2020. https://www.agenformedia.com/wp-content/uploads/2020/10/Technology1_VCinelli.pdf.

Clark, D.D., *Characterizing cyberspace: Past, present and future*, ECIR Working Paper, 2010, 3, MIT Political Science Department.

Cordner, G., Scott, M.S., *Police Discretion and Its Control*, in G. Bruinsma, D. Weinsburd (a cura di), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, pp. 3587-3596.

Couldry, N., Mejias, U.A., *The decolonial turn in data and technology research: what is at stake and where is it heading?*, in *Information, Communication & Society*, 2023, 26(4), pp. 786-802.

Courtland, R., *Bias detectives: The researchers striving to make algorithms fair*, in *Nature*, 2018, 558(7710), pp. 357-360.

Crenshaw, K., *Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color*, in *Stanford Law Review*, 1991, 43(6), pp. 1241-1299.

Dal Lago, A., *Non-persone*, Milano, Feltrinelli, 1999.

D'Angelo, G., Giacomello, G., *Cybersicurezza. Che cos'è e come funziona*, Bologna, il Mulino, 2023.

Danziger, S., Levav, J., Avnaim-Pesso, L., *Extraneous factors in judicial decisions*, in *Proceedings of the National Academy of Sciences*, 2011, 108(17), pp. 6889-6892.

DeKeseredy, W.S., Perry B. (a cura di), *Advancing Critical Criminology: Theory and Application*, Lanham (MD), Lexington Books, 2006.

Desrosières, A., *The Politics of Large Numbers: A History of Statistical Reasoning*, Cambridge (MA), Harvard University Press, 2002.

Di Nicola, A., *Criminalità e criminologia nella società digitale*, Milano, FrancoAngeli, 2021.

Dubber, M.D., Valverde, M., *Perspectives on the power and science of police*, in M.D. Dubber, M. Valverde (a cura di), *The New Police Science: The Police Power in Domestic and International Governance*, Stanford, Stanford University Press, 2006.

Egbert, S., Krasmann, S., *Predictive policing: not yet, but soon preemptive?*, in *Policing and Society*, 2020, 30(8), pp. 905-919.

Egbert, S., Leese, M., *Criminal Futures: Predictive Policing and Everyday Police Work*, London-New York, Routledge, 2021.

Entman, R.M., *Framing: Towards clarification of a fractured paradigm*, in *Journal of Communication*, 1993, 43, pp. 51-58.

Epp, C.R., Maynard-Moody, S., Haider-Markel, D.P., *Pulled Over: How Police Stops Define Race and Citizenship*, Chicago Series in Law and Society, Chicago, University of Chicago Press, 2014.

Erichsen Skjevrak, P., Gundhus, H.O.I., *From personal archives to intelligence: Visibility and ignorance in forecasting "youth at risk"*, in V. Galis, H.O.I. Gundhus, A. Vradis (a cura di), *Critical Perspectives on Predictive Policing*, Cheltenham-Northampton, Edward Elgar Publishing, 2025, pp. 63-83.

Fabini, G., *Il sapere sulla polizia*, in G. Fabini, E. Gargiulo, S. Tuzza, *Polizia: Un vocabolario dell'ordine*, Milano, Mondadori Università, 2023.

Fabini, G., *Polizia e migranti in città: negoziare il confine nei contesti locali*, Roma, Carocci, 2022.

Fabini, G., Gargiulo, E., Tuzza, S., *Discrezionalità*, in G. Fabini, E. Gargiulo, S. Tuzza, *Polizia: un vocabolario dell'ordine*, Milano, Mondadori Università, 2023, pp. 127-135.

Fabini, G., Gargiulo, E., Tuzza, S., *Polizia: un vocabolario dell'ordine*, Milano, Mondadori Università, 2023.

Feeley, M.M., Simon, J., *The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications*, in *Criminology*, 1992, 30(4), pp. 449-474.

Ferguson, G., *The Rise of Big Data Policing. Surveillance, race and the future of law enforcement*, New York, New York University Press, 2017.

Firouzi Tabar, O., *Una rassegna di ricerche sulla percezione dell'insicurezza in Italia: forza e vulnerabilità del "paradigma sicuritario"*, in *Studi sulla questione criminale*, 2014, 3, pp. 73-92.

Floridi, L., *The onlife manifesto: Being human in a hyperconnected era*, Springer International Publishing, 2015.

Floridi, L., *The Ethics of Information*, Oxford, Oxford University Press, 2013.

Foucault, M., *Nascita della biopolitica. Corso al Collège de France (1978-1979)*, Milano, Feltrinelli, 2005.

Foucault, M., *Sicurezza, territorio, popolazione. Corso al Collège de France (1977-1978)*, Milano, Feltrinelli, 2005.

Foucault, M., *La volontà di sapere*, Milano, Feltrinelli, 1978.

Foucault, M., *Sorvegliare e punire. Nascita della prigione*, Torino, Einaudi, 1976.

Friedman, T., *It's a 401(k) world*, in *The New York Times*, 1 maggio 2013.

Furnell, S., *Cybercrime: Vandalizing the information society*, Addison, Wesley, 2002.

Furnell, S., *The problem of categorising cybercrime and cybercriminals*, 2nd Australian Information Warfare and Security Conference, Perth, Australia, 2001

Furnell, S., *The evolving landscape of technology-dependent crime*, in M.R. McGuire, T. Holt (a cura di), *The handbook of technology, crime and justice*, Abingdon, Routledge, 2017.

Fussey, P., Roth, S., *Digitizing the Governance of Security Infrastructure: Big Data, Predictive Analytics and Surveillance*, in *Surveillance & Society*, 2020, 18(2), pp. 204-221.

Galis, V., Oppen Gundhus, H., Vradis, A., *Critical Perspectives on Predictive Policing: Anticipating Proof?*, Cheltenham-Northampton, Edward Elgar Publishing, 2025, pp. 6-7.

Garante per la protezione dei dati personali, *Provvedimento n. 207 del 10 novembre 2022: Linee guida sui trattamenti di dati personali per finalità di intelligenza artificiale. Garante per la protezione dei dati personali*, 2022. https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9977020.

Gargiulo, E., *La Parola e la cosa*, in G. Fabini, E. Gargiulo, S. Tuzza, *Polizia: un vocabolario dell'ordine*, Milano, Mondadori Università, 2023.

Ghernauti, S., *Cyber Power: crime, conflict and security in cyber space*, EFPL Pess, CRC Press, 2013.

Gialuz, M., Quattrocolo, S., *AI and the administration of criminal justice in Italy (A-01-23)*, Penal, 2023. https://www.penal.org/sites/default/files/files/A-01-23.pdf-

Gitelman, L. (a cura di), *Raw Data Is an Oxymoron*, Cambridge (MA), MIT Press, 2013.

Giupponi, T.F., *Il governo nazionale della cybersicurezza*, in *Quaderni Costituzionali*, (2), 2024.

Glouftsios, G., Leese, M., *Epistemic fusion: Passenger Information Units and the making of international security*, in *Review of International Studies*, 2023, 49(1), pp. 125-142.

Goldstein, J., *Police Discretion not to Invoke the Criminal Process: Low Visibility Decisions in the Administration of Justice*, in *Yale Law Journal*, 1960, 69, pp. 543-594.

Gordon, S., Ford, R., *On the definition and classification of cybercrime*, in *Journal in Computer Virology*, 2006, pp. 13-20.

Gundhus, H.O.I., Jansen, P.T., *Pre-crime and policing of migrants: Anticipatory action meets management of concerns*, in *Theoretical Criminology*, 2019, pp. 1-20.

Haggerty, K., Ericson, R., *The surveillant assemblage*, in *British Journal of Sociology*, 2000, 4, pp. 605-622.

Hand, D. J., Mannila, H., Smyth, P., *Principles of Data Mining*, Cambridge (MA), MIT Press, 2001.

Hannah-Moffat, K., *Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates*, in *Theoretical Criminology*, 2018, 23(4), pp. 453-470.

Harcourt, B.E., *Risk as a Proxy for Race: The Dangers of Risk Assessment*, in *Federal Sentencing Reporter*, 2015, 27, pp. 237-243.

Hillyard, P., Pantazis, C., Tombs, S., Gordon D. (a cura di), *Beyond Criminology: Taking Harm Seriously*, London, Pluto Press, 2004.

Holt, T., *Crime on-line: Correlates, causes, and context*, Durham, Carolina Academic Press, 2013.

Holt, T., Bossler, A., Seigfried-Spellar, K., *Cybercrime and digital forensics. An Introduction*, Abingdon, New York, Routledge, 2022.

Horst, H., Miller, D., *The digital and the human: A prospectus for digital anthropology*, in H. Horst, D. Miller (a cura di), *Digital Anthropology*, New York, Berg, 2013, p. 5.

Jaishankar, K., *Space transition theory of cyber crimes*, in F. Schmallager, M. Pittaro (a cura di), *Crimes of the internet*, Upper Saddle River, NJ, Prentice Hall, pp. 283-301.

Jasanoff, S., *Future imperfect: Science, technology, and the imaginations of modernity*, in S. Jasanoff, S.H. Kim (a cura di), *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*, Chicago, University of Chicago Press, 2015.

Jasanoff, S., Kim, S.H., Sperling, S., *Sociotechnical Imaginaries and Science and Technology Policy: A Cross-National Comparison*, 2007. https://stsprogram.org/admin/files/imaginaries/NSF-imaginaries-proposal.pdf.

Jewkes, Y., Yar, M., *Handbook of internet crime*, Devon, Willan Publishing, 2013.

Karlsson, B., Galis, V., *POL-INTEL: Predictive policing and the politics of data integration in Denmark*, in V. Galis, H.O.I. Gundhus, A. Vradis (a cura di), *Critical Perspectives on Predictive Policing*, Cheltenham-Northampton, Edward Elgar Publishing, 2025, pp. 84-103.

Kaufmann, M., *AI in policing and law enforcement*, in *Handbook on Public Policy and Artificial Intelligence*, Cheltenham-Northampton, Edward Elgar Publishing, 2024, pp. 295-304.

Kaufmann, M., Egbert, S., Leese, M., *Predictive policing and the politics of patterns*, in *British Journal of Criminology*, 2019, 59(3), pp. 674-692.

Kaufmann, M., Leese, M., *Information In-Formation: Algorithmic Policing and the Life of Data*, in V. Badalič, A. Završnik (a cura di), *Automating Crime Prevention, Surveillance, and Military Operations*, Cham, Springer, 2021, pp. 69-83.

Kaufmann, M., Lomell, H., *De Gruyter Handbook of Digital Criminology*, Berlin, De Gruyter, 2025.

Kitchin, R., *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*, Los Angeles, London, New Delhi, Singapore, Washington D.C., Sage, 2014.

Krasmann, S., *The enemy on the border: Critique of a programme in favour of a preventive state*, in *Punishment and Society*, 2007, 9(3), pp. 301-318.

Kusak, M., *Quality of data sets that feed AI and big data applications for law enforcement*, in *ERA Forum*, 2022, 23(2), pp. 209-219.

Latour, B., *Reassembling the Social: An Introduction to Actor-Network-Theory*, Oxford, Oxford University Press, 2005.

Latour, B., *Science in Action: How to Follow Scientists and Engineers Through Society*, Cambridge (MA), Harvard University Press, 1987.

Lavorgna, A., Ugwudike, P., *The datafication revolution in criminal justice: An empirical exploration of frames portraying data-driven technologies for crime prevention and control*, in *Big Data and Society*, 2021, 8(2).

Leman-Langlois, S., *Technocrime: Policing and surveillance*, London, Routledge, 2014.

Lipsky, M., *Street-Level Bureaucracy: Dilemmas of the Individual in Public Service*, New York, Russell Sage Foundation, 1980.

Lupton, D., *Digital Sociology*, London, Routledge, 2015.

Lustgarten, L., *The Governance of Police*, London, Sweet and Maxwell, 1986.

Lyon, D., *Surveillance studies: An overview*, Cambridge, Polity Press, 2007.

Mann, D., Sutton, M., *Netcrime: More change in the organization of thieving*, in *British Journal of Criminology*, 1998, (2), pp. 201-229.

Manning, P.K., *Police Work*, Cambridge (MA), The MIT Press, 1977.

Manyika, J., *et al*., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, McKinsey Global Institute, giugno 2011.

Marchant, R., *Bayesian techniques for modelling and decision-making in criminology and social sciences*, presentazione alla conferenza *Automated Justice: Algorithms, Big Data and Criminal Justice Systems*, Collegium Helveticum, Zürich, 20 aprile 2018. https://collegium.ethz.ch/wp-content/uploads/2018/01/180420_automated_justice.pdf.

Mastrobuoni, G., *Crime is Terribly Revealing: Information Technology and Police Productivity*, in *The Review of Economic Studies*, 2020, 87(6), pp. 2727-2753.

Mattes, G., *Predictive policing in Sweden*, in V. Galis, H.O.I. Gundhus, A. Vradis (a cura di), *Critical Perspectives on Predictive Policing*, Cheltenham-Northampton, Edward Elgar Publishing, 2025, pp. 165-183.

Matthewman, S., *Technology and Social Theory*, Basingstoke, Palgrave Macmillan, 2011.

Mayer, M., Gabrielli, F., *Next generation Eu: The digital transition's policy dilemmas*, in *Rivista di Digital Politics*, 2022, 3, pp. 1-22.

Mayer-Schönberger, V., Cukier, K., *Big Data: A Revolution That Will Transform How We Live, Work and Think*, London, John Murray, 2013.

McGuire, M., *It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime*, in R. Leukfeldt, T. Holt (a cura di), *The human factor of cybercrime*, New York, Routledge, 2020, pp. 3-28.

McGuire, M.R., *Hypercrime: The new geometry of harm*, London, Routledge, 2008;

McLuhan, M., Fiore, Q., *The medium is the massage: An inventory of effects*, San Francisco (CA), Hardwired, 1967.

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

Melossi, D., *1977, da Bologna a Berkeley*, in *Studi Sulla Questione Criminale*, 2013, 3, pp. 39-44.

Melossi, D., *Stato, controllo, devianza*, Bologna, il Mulino, 2002.

Milivojevic, S., *Crime and Punishment in the Future Internet: Digital Frontier Technologies and Criminology in the Twenty-First Century*, Abingdon, New York, Routledge, 2021

Morozov, E., *To Save Everything, Click Here: The Folly of Technological Solutionism*, New York, PublicAffairs, 2013.

Neiva, L., Granja, R., Machado, H., *Big Data applied to criminal investigations: expectations of professionals of police cooperation in the European Union*, in *Policing and Society*, 2022, 32(10), pp. 1167-1179.

Neiva, L., Machado, H., Silva, S., *The views about Big Data among professionals of police forces: A scoping review of empirical studies*, in *International Journal of Police Science and Management*, 2023, 25(2), pp. 208-220.

Neocleous, M., *The Fabrication of Social Order: A Critical Theory of Police Power*, London, Pluto Press, 2000.

Neresini, F., *Quando i numeri diventano grandi: che cosa possiamo imparare dalla scienza*, in *Rassegna Italiana di Sociologia*, 2015, 56(3-4), pp. 405-431.

Neroni Rezende, I., *Facial Recognition for Preventive Purposes: the Human Rights Implications of Detecting Emotions in Public Spaces*, in L. Bachmaier Winter, S. Ruggeri (a cura di), *Investigating and Preventing Crime in the Digital Era*, Cham, Springer, 2022, pp. 67-98.

Newburn, T., Reiner, R., *Policing and the Police*, in M. Maguire, R. Morgan, R. Reiner (a cura di), *The Oxford Handbook of Criminology*, 5ª ed., Oxford, Oxford University Press, 2012

O'Neil, C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, Crown Random House, 2016.

Ongaro, F., Simonini, B., *Software italiano Giove per la polizia predittiva: Pro e contro*, in *Agenda Digitale*, 5 settembre 2023. https://www.agendadigitale.eu/documenti/giustizia-digitale/ia-in-polizia-e-giustizia-predittiva-opportunita-e-rischi-del-software-italiano-giove.

Papada, E., Vradis, A., *The birth of spatial transgression: genealogies and regulatory instruments in the use of facial recognition technologies in the UK*, in V. Galis, H.O.I. Gundhus, A. Vradis (a cura di), *Critical Perspectives on Predictive Policing: Anticipating Proof?*, Cheltenham-Northampton, Edward Elgar Publishing, 2025, pp. 43-64.

Pegasoft s.r.l., *Polizia predittiva, il software Giove prevedrà reati e omicidi*, Pegasoft S.r.l., 2023. https://www.pegasoftsrl.it/polizia-predittiva-il-software-giove-prevedra-reati-e-omicidi/

Phillips, C., Bowling, B., Parmar, A., *Ethnicities, racism, crime and criminal justice,* in A. Liebling, S. Maruna, L. McAra (a cura di), *The Oxford Handbook of Criminology*, Oxford, Oxford University Press, 2023.

Pietrangelo, M., *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista Italiana di Informatica e Diritto*, 2024, (2), pp. 13-24.

Pietrocarlo, D.E., *La predictive policing nel regolamento europeo sull'intelligenza artificiale*, in *La Legislazione Penale*, 2024, pp. 1-35.

Powel, A., Stratton, G., Cameron, R., *Digital criminology. Crime and justice in digital society*, Abingdon, Oxon, Routledge, 2018.

Privacy Network, *Amministrazione automatizzata. Report 2024/2025*, 2025. https://media.privacy-network.it/privacynetwork/uploads/2025/05/report-osservatorio-OAA.pdf.

ProPublica, *COMPAS recidivism risk score data and analysis*, 2017. https://www.propublica.org/datastore/dataset/compas-recidivism-risk-score-dataand-analysis.

Quan-Haase, A., Wellman, B., *Hyperconnected net work: Computer-mediated community in a high-tech organization*, in C. Heckscher, P. Adler (a cura di), *The firm as a collaborative community: Reconstructing trust in the knowledge economy*, New York (NY), Oxford University Press, 2006, pp. 281-333.

Quassoli, F., *"Clandestino": Institutional discourses and practices for the control and exclusion of migrants in contemporary Italy*, in *Journal of Language and Politics*, 2013, 12(2), pp. 203-225.

Quassoli, F., *Il sapere dei magistrati: un approccio etnografico allo studio delle pratiche giudiziarie*, in A. Dal Lago, R. De Biasi (a cura di), *Un certo*

sguardo. Introduzione all'etnografia sociale, Roma-Bari, Laterza, 2002, pp. 196-217.

Quassoli, F., Chiodi, M., *Rappresentazioni sociali e pratiche organizzative di polizia e magistratura*, in *Quaderno n. 21 di Città Sicure*, Regione Emilia-Romagna, 2000, pp. 117-293.

Reiner, R., *The Politics of the Police*, Oxford, Oxford University Press, 2000.

Richardson, R., Schultz, J.M., Crawford, K., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, in *NYU Law Review Online*, 2019, 94, pp. 192-233.

Rosso, E., *Cosa sappiamo di Giove, l'algoritmo con cui la polizia italiana vuole prevedere i reati*, Fanpage.it, 7 giugno 2023. https://www.fanpage.it/innovazione/tecnologia/cosa-sappiamo-di-giove-lalgoritmo-con-cui-la-polizia-italiana-vuole-prevedere-i-reati/

Ruppert, E., Isin, E., Bigo, D., *Data politics*, in *Big Data & Society*, 2017, 4(2), pp. 1-7.

Sartori, L., *Digital Divide. Le nuove disuguaglianze nella società dell'informazione*, Bologna, il Mulino, 2006.

Sbraccia, A., *Criminologie post-coloniale*, in C. Rinaldi, P. Saitta (a cura di), *Criminologie critiche contemporanee*, Milano, Giuffrè Francis Lefebvre, 2018, pp. 27-49.

Schuilenburg, M., Soudijn, M., *Big data policing in the Netherlands: The politics of unpredictability*, in *European Journal of Criminology*, 2023, 20(2), pp. 246-264.

Selmini, R., *Dalla sicurezza urbana al controllo del dissenso politico. Una storia del diritto amministrativo punitivo*, Roma, Carocci, 2020.

Senato della Repubblica, *Legislatura 19ª - Atto di Sindacato Ispettivo n. 3-00499*, Senato, 13 giugno 2023. https://www.senato.it/show-doc?id=1378767&leg=19&tipodoc=Sindisp.

Sguazzini, M., *Privacy politics: Power relations in the extraction, management, and use of personal data by non-state actors*, in *Rivista di Digital Politics*, 2022, II(3), pp. 399–422.

Signorelli, A.D., *Perché la più avanzata startup italiana di polizia predittiva è sull'orlo del baratro*, Wired Italia, 31 gennaio 2024. https://www.wired.it/article/polizia-predittiva-keycrime-startup-ai-act/

Skolnick, J. H., *Justice without Trial: Law Enforcement in Democratic Society*, New York-London-Sydney, John Wiley and Sons, 1966.

Smith, P., O'Malley, G.J.D., *Driving politics: Data-driven governance and resistance*, in *British Journal of Criminology*, 2017, 57(2), pp. 275-298.

Solove, D. J., *Understanding Privacy*, Cambridge (MA), Harvard University Press, 2008.

Solove, D. J., *A taxonomy of privacy*, in *University of Pennsylvania Law Review*, 2006, 154(3), pp. 477-560.

Steinmetz, K.F., *Against Cybercrime. Towards a Realist Criminology of Computer Crimes*, Abingdon, Routledge, 2024.

Stratton, G., Powell, A., Cameron, R., *Crime and justice in digital society: Towards a 'digital criminology'?*, in *International Journal for Crime, Justice and Social Democracy*, 2017, 6, 2, pp. 17-33.

Taylor, P. Walton, J. Young, *The New Criminology: For a Social Theory of Deviance*, London-New York, Routledge, 1973.

Tazzioli, M., *The Making of Migration: The Biopolitics of Mobility at Europe's Borders*, London, SAGE Publications, 2020.

Thomas, D., Loader, I., *Cybercrime: law enforcement, security and surveillance in the information age*, London, Routledge, 2000.

Tuzza, S., *Il dito e la luna*, Torino, Piemme Edizioni, 2021.

Ursi, R. (a cura di), *La sicurezza nel cyberspazio*, Milano, Franco Angeli, 2023.

Van Brakel, R., Govaerts, L., *Exploring the impact of algorithmic policing on social justice: Developing a framework for rhizomatic harm in the pre-crime society*, in *Theoretical Criminology*, 2024, 29(1), pp. 91-109.

Van Brakel, R., Meijer, A., *Predictive Policing: The Role of Big Data in Policing*, in *Information Polity*, 2018, 23(3), pp. 222-234.

Van Dijk, J., *Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology*, in *Surveillance & Society*, 2014, 12(2), pp. 197-208.

Van Dijk, J., *The Deepening Divide: Inequality in the Information Society*, Thousand Oaks, Sage, 2005.

Vesla, M., Andrew Papachristos, W., Zanger-Tishler, M., *The Great Decoupling: The Disconnection between Criminal Offending and Experience of Arrest across Two Cohorts*, in *RSF: The Russell Sage Foundation Journal of the Social Sciences*, 2019, 5, 1, pp. 89-123.

Vitale, C., *Networkologies: A philosophy of networks for a hyperconnected age*, Alresford (UK), Zero Books, 2014.

Waddington, P.A.J., *Policing Citizens. Authority and Rights*, London, UCL Press, 1999.

Wall, D., *How big data feeds big crime*, in *Global His. J. Contemp. World Aff.*, January 2018, pp. 29-34.

Wall, D., *Crime and the internet*, in D. Wall (a cura di), *Crime and the internet*, Abingdon, Routledge, 2001, pp. 1-17.

Wall, D.S., *Digital realism and the governance of spam as cybercrime*, in *European Journal on Criminal Policy and Research*, 2005, 10, 4, pp. 309-335.

Wall, D.S. (a cura di), *Cyberspace crime*, London, Routledge, 2003.

Walton, P., Young, J., *The New Criminology Revisited*, in P. Walton, J. Young (a cura di), *The New Criminology Revisited*, London, Palgrave Macmillan, 1998, p. vii.

Weber, L., Bowling, B., *Stop and search in global context*, in *Policing and Society*, 2016, 21(4), pp. 353-356.

Willoughby, A., Nellis, M., *"You cannot really hide": Experiences of probation officers and young offenders with GPS tracking in Winnipeg, Canada*, in *Journal of Technology in Human Services*, 2016, 34(1), pp. 63-81.

Wilson, J.Q., *Varieties of Police Behaviour*, Cambridge (MA), Harvard University Press, 1968.

Wonders, N.A., *Global Flows, Semi-permeable Borders and New Channels of Inequality*, in L. Weber, S. Pickering (a cura di), *Borders, Mobility and Technologies of Control*, Dordrecht, Springer, 2006, pp. 63-86.

Yar, M., *Cybercrime and society,* London, Sage, 2006.

Završnik, A., *Big Data*, in M. Kaufmann, H.M. Lomell (a cura di), *De Gruyter Handbook of Digital Criminology*, Berlin-Boston, De Gruyter, 2025, pp. 107-114.

Završnik, A., *Algorithmic justice: Algorithms and big data in criminal justice settings*, in *European Journal of Criminology,* 2019, 18, 5, pp. 632-642.

Zuboff, S., *Big other: Surveillance capitalism and the prospects of an information civilization*, in *Journal of Information Technology*, 15, 3, 2015, pp. 75-89.

Zuboff, S., *In the age of the smart machine: The future of work and power*, New York, Basic Books, 1988.

Finito di stampare nel mese di dicembre 2025
per i tipi di Bologna University Press