

Gabriele Suffia (Università degli Studi di Bologna),
Anita Lavorgna (Università degli Studi di Bologna
e Università di Southampton)** , Simone Icardi
(Ontario Tech University)****

POLIZIA “SMART” TRA PAURE E REALTÀ: UN’ANALISI ESPLORATIVA SULLA RAPPRESENTAZIONE MEDIATICA DELLO SMART POLICING IN ITALIA

1. Introduzione. – 2. La sfida di essere “smart” nell’era dei dati digitali (o digitalizzati). – 3. La datificazione della sicurezza. – 3.1. Le promesse della giustizia algoritmica. – 3.2. Approcci critici. – 3.3. Il nostro contributo. – 4. Metodologia. – 5. Analisi e discussione. – 5.1. Il quando e il dove dello *smart policing* nella rappresentazione mediatica. – 5.2. Il cosa e il come dello *smart policing* nella rappresentazione mediatica. – 6. Note conclusive e nuove prospettive di ricerca.

1. Introduzione

La datificazione è un fenomeno in rapida proliferazione nelle società contemporanee, e può essere definita come la «quantificazione onnipresente della vita sociale» (S. Baack, 2015, 2). Sempre più utilizzata per informare i processi decisionali nei settori pubblici, politici ed economici, la datificazione all’atto pratico si manifesta principalmente nell’analisi dei *big data*. Essa nasce originariamente dalla cosiddetta “rivoluzione dei dati” (Nazioni Unite, 2014) avvenuta negli ultimi decenni e specialmente in seguito alla commercializzazione del cyberspazio (si pensi alla mole di dati prodotti da ogni nostra interazione digitale). Non va però dimenticato come la datificazione odierna sia anche un prodotto dell’accumulo passato di dati amministrativi su larga scala, ora fruibili e analizzabili con strumenti automatizzati (D. Boyd, K. Crawford, 2012). Inoltre, sempre più stiamo assistendo al tentativo di generare grandi moli di dati a partire da realtà sociali “fisiche” sempre più digitalizzate (es., nell’ambito urbano con le tecnologie delle cosiddette smart cities – per una discussione critica sul punto, si veda McGuire, 2018), al fine

* Dottorando in Law, Science and Technology presso l’Alma Mater Studiorum, Università degli Studi di Bologna.

** Professoressa associata, Dipartimento di Scienze politiche e sociali, Università degli Studi di Bologna. Fino a settembre 2022 professoressa associata di Criminologia nel Department of Sociology Social Policy & Criminology dell’Università di Southampton (Regno Unito).

*** Dottorando in Criminology and Social Justice presso l’Ontario Tech University (Canada).

di registrare una serie di eventi e azioni e, successivamente, analizzare e processare i dati (S.E. Bibri, 2019).

La datificazione ha una rilevanza diretta anche in ambiti sensibili come quello della sicurezza, e, come vedremo a breve, negli ultimi anni un numero crescente di studi accademici ne ha presentato potenzialità e criticità. Questi processi di datificazione hanno lentamente preso piede anche nel dibattito pubblico, e non è raro ormai imbattersi in notizie che affrontano questa tematica. Non dovrebbe, dunque, sorprendere come la rappresentazione mediatica di questo fenomeno sia di grande rilevanza socio-criminologica, in quanto la percezione che il pubblico generale ha di fenomeni complessi (come quello della datificazione) tende a dipendere da come questi vengono rappresentati da fonti mediatiche di largo consumo (C. Sofia, 2004; F. Tonello, 2008; A. Coluccia *et al.*, 2014; G. Tipaldo, 2014): è stato studiato a lungo, ad esempio, come le rappresentazioni mediatiche informino e influenzino le percezioni di cosa sia un problema, o quali siano i modi migliori per cercare di risolverlo (S. Cohen, 1972; T. Bennet *et al.*, 1982; E. Burney, 2009; R. Surette, K. Kampe, 2016). Del resto, in linea con gli insegnamenti della criminologia culturale, le rappresentazioni mediatiche della criminalità ma anche della sicurezza sono rappresentazioni *mediate*, di grande interesse per la disciplina in quanto alla base di ogni raffronto critico con le politiche alla base di tali rappresentazioni (J. Ferrell, 2013).

A partire da tali premesse, il nostro contributo si propone di offrire un'analisi esplorativa di come l'avvento della datificazione nel settore della sicurezza sia stato accolto nell'ambito mediatico italiano, focalizzandosi in particolare sul settore del cosiddetto *smart policing* – i.e., l'uso anti-criminalità e pro-sicurezza da parte delle forze di polizia di una serie di tecnologie *smart*, ossia considerate intelligenti in quanto permetterebbero di ottimizzare e migliorare processi esistenti grazie all'utilizzo di algoritmi¹.

¹ Va precisato come il concetto di *smart policing*, sebbene sia emerso come un paradigma indipendente nell'ambito degli studi sulle forze di polizia e di sicurezza nell'ultimo decennio (J.R. Coldren *et al.*, 2013), sia ovviamente connesso ad altri paradigmi presenti in letteratura. Vi sono sovrapposizioni con il cosiddetto *intelligence-led policing* (J.H. Ratcliffe, 2016) in quanto l'analisi dei dati è in entrambi i modelli alla base delle scelte operative e decisionali (ma l'*intelligence-led policing* potrebbe non basarsi su algoritmi, quindi non essere "smart"; inoltre, l'ambito di operatività dello *smart policing* è più ampio, non essendo univocamente legato alle teorie criminologiche delle opportunità criminali, e non prioritizzando necessariamente *hot spots*, rivittimizzazioni, o criminali prolifici, J.H. Ratcliffe, 2008). Importanti sono anche i punti di contatto con la polizia predittiva (*predictive policing*, M. Kaufmann *et al.*, 2019; A.J. Meijer, M. Wessels, 2019), al punto che "smart" e "predittivo" vengono talvolta utilizzati, impropriamente, come fossero sinonimi, mentre la funzione predittiva è solo uno degli ambiti di utilizzo dello *smart policing*.

2. La sfida di essere “smart” nell’era dei dati digitali (o digitalizzati)

Prima di offrire una breve revisione della letteratura esistente sulla datificazione nell’ambito della sicurezza, si ritiene utile aprire una breve parentesi per chiarire cosa ci sia alla base del concetto di *smart*, termine che connota gli approcci di polizia al centro di questo studio. Questi sono principalmente approcci di Intelligenza Artificiale (IA), categoria con cui si definiscono le tecnologie alla base di sistemi in grado di analizzare il proprio ambiente e compiere azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi (Commissione Europea, 2018; G. Finocchiaro, 2019). Va rilevato come non vi sia un *continuum* necessario tra fenomeni di datificazione e l’utilizzo di IA (l’IA funziona usando ampie moli di dati, ma ampie moli di dati di per sé non generano IA); tuttavia, ai fini di questo contributo, si ritiene utile sottolineare la convergenza tra queste due tematiche, in quanto le tecnologie “smart” al centro della nostra analisi derivano direttamente dalla disponibilità e abbondanza di dati. Tecnologie “smart” di questo tipo sono state utilizzate in maniera incrementale nelle nostre società già da una cinquantina di anni, con effetti trasformativi (E. Esposito, 2013; R. Gruetzemacher, J. Whittlestone, 2019). Nell’ambito della sicurezza e della giustizia penale, il cosiddetto *smart policing* è senza dubbio il settore che ha ricevuto maggiore attenzione fino ad ora, con sistemi di IA che vengono sempre più utilizzati, in molti Stati, per “prevedere” – tra le altre cose – fattori di rischio, hotspot criminali o per implementare identificazioni biometriche, generalmente al fine di allocare al meglio le risorse di polizia disponibili (J. Chan, L. Bennet Moses, 2017; G. Mastrobuoni, 2020).

Semplificando, tra le tecnologie più utilizzate dall’IA troviamo il *data mining* (l’estrazione in maniera automatica o semi-automatica di informazioni da grossi dataset), il *natural language processing* (l’elaborazione del linguaggio naturale o NLP, ovvero quella applicazione dell’IA che si occupa di fornire ad algoritmi informatici la capacità di comprendere ed elaborare il contenuto di una comunicazione umana), la *sentiment analysis* (la rilevazione a valutazione automatica di determinati contenuti di comunicazioni umani), e il *machine learning* (la capacità dell’algoritmo di apprendere, imparando ad approssimare al meglio la funzione di relazione tra variabili per inferire pattern nascosti in grandi moli di dati). Come si può facilmente notare, ognuna di queste tecnologie ha come base di partenza il dato (di tipo biometrico, demografico, economico, o altro) che, come il petrolio, viene estratto, registrato, raccolto e venduto, in un vero e proprio mercato (A. De Franceschi, M. Lehmann, 2015; M. Borghi, 2018). Come per il petrolio, anche nel mondo digitale bisogna fare i conti con chi detiene il controllo del bene prezioso: vi sono i colossi che primeggiano nel mercato dei dati (da Facebook a Twitter,

passando per Amazon e Google), ma anche aziende di medie dimensioni che si occupano di sicurezza informatica, banche, tribunali, e via dicendo. A questi bisogna aggiungere tutte quelle sotto-strutture dedicate alla creazione e immagazzinamento dei dati che vengono dalle tecnologie *smart*: si pensi ai sensori, agli strumenti di videosorveglianza o anche solo alle celle che offrono wi-fi gratuito disponibili in molte delle nostre città.

3. La datificazione della sicurezza

3.1. Le promesse della giustizia algoritmica

Negli ultimi anni, una serie di ricerche si sono occupate delle possibilità offerte dall'uso dei *big data* in combinazione ad approcci di IA in settori come quello della sicurezza e della giustizia penale. Se per motivi di spazio non è possibile offrire in questo contesto una panoramica dettagliata², vogliamo tuttavia puntualizzare come per molto tempo un ampio *corpus* di letteratura, specie nell'ambito dello *smart policing*, si sia principalmente concentrato sui miglioramenti della tecnica e sulle nuove possibilità offerte dalla tecnologia.

Va sottolineato come sia il settore privato, sia il mondo della ricerca (specie nell'ambito dell'informatica e statistica, quindi in quei settori che primeggiano in termini di capitale digitale, ma spesso manchevoli di capitale intellettuale e critico su tematiche di interesse socio-criminologico, si veda J. Van Dijk, 2005) siano tradizionalmente stati in prima linea nello sviluppo dei modelli algoritmici alla base degli odierni fenomeni di datificazione. Per quanto riguarda in particolare lo *smart policing*, numerosi studi si sono occupati di come ottimizzare l'utilizzo delle (scarse) risorse umane nel decidere quali zone urbane monitorare con maggiore attenzione (tra i numerosi studi sul punto, si veda M. Camacho-Collados, F. Liberatore, 2015; F. Leuzzi *et al.*, 2018; J. Leigh *et al.*, 2019), o di come migliorare pratiche di sorveglianza e monitoraggio sia offline che online. Come analizzato da S. Brayne (2017), nella pratica la datificazione applicata alle forze di polizia ha già trasformato, almeno in parte, le pratiche di sorveglianza, non solo amplificandole da un punto di vista quantitativo, ma anche modificandole qualitativamente, in quanto – tra le altre cose – le valutazioni discrezionali del rischio sono ora spesso integrate e quantificate utilizzando appositi punteggi (*risk scores*); la predizione, più che la reazione, diventa spesso centrale; nelle banche dati utilizzate rientrano anche persone che non hanno avuto contatti diretti pre-

² Per una revisione della letteratura più dettagliata, si rimanda *e.g.* a F. Basile (2019); R. Brownsword, A. Harel (2019); A. Lavorgna, P. Ugwu-dike (2021).

cedenti con la polizia. Si rileva inoltre che, se all'inizio le tecnologie *smart* si ponevano in un ruolo di supporto, ausiliario, alle forze di polizia, certi approcci di IA di nuova generazione tendono a promettere, e offrire, la possibilità di prendere anche decisioni complesse con un grado significativo di autonomia (B. Benbouzid, 2019).

Nel complesso, una parte della letteratura si è comunque mostrata tendenzialmente ottimista nei confronti delle possibilità offerte dalle nuove tecnologie e dalla disponibilità di grosse quantità di dati anche in ambiti “sensibili” come quello della sicurezza e della giustizia penale (A. Lavorgna, P. Ugwu-dike, 2021), conseguentemente evocando e legittimando immaginari sociotecnici (S. Jasanoff *et al.*, 2007) positivi. È stato riportato come questi immaginari positivi di approcci *smart* siano diventati in certi contesti immaginari collettivi, sostenuti dai decisori politici, e da parti della cittadinanza (*ivi*), con la conseguenza che vi sono aspettative pubbliche, su alcuni servizi basati su algoritmi, che tendono a sopravvalutare le potenzialità delle tecnologie in uso (J.S. Hollywood *et al.*, 2018; A. Lavorgna, P. Ugwu-dike, 2021)³.

3.2. Approcci critici

Specialmente in ambito internazionale vi è, però, una letteratura, in rapida crescita, critica sulla proliferazione della datificazione in ambito di polizia e sicurezza (tra i molti, si vedano J. Angwin, J. Larson, 2016; S. Barocas, A.D. Selbst, 2016; D. Ensign *et al.*, 2018; A. Ferguson, 2017; K. Lum, W. Isaac, 2016; L. Bennet Moses, J. Chan, 2018; K. Hannah-Moffat, 2018; P. Fussey, D. Murray, 2019; A. Lavorgna, P. Ugwu-dike, 2021). Questo filone di ricerca critica rifiuta gli immaginari sociotecnici positivi menzionati precedentemente, e a questi contrappone immaginari più complessi, che riconoscono come i *big data* e gli approcci di IA su di essi basati non siano sempre facili da gestire, non possano offrire certezze, ma solo proiezioni basate su modelli computazionali, e possano altresì creare danni sociali di rilievo significativo – i cosiddetti *tech harms* (B.H.M. Custers, 2013; A. Iliadis, F. Russo, 2016; A. Lavorgna, P. Ugwu-dike, 2021; M.A. Wood, 2021). Basarsi su dati amministrativi del passato per formare gli algoritmi, ad esempio, rischia di replicare, in un circolo vizioso, disuguaglianze sociali “storiche” esistenti e persistenti, come quelle basate su genere, etnia e status socioeconomico (si vedano S. Starr, 2014; Law Society, 2019; A. Završnik, 2021; P. Ugwu-dike, 2020). Una serie di studi ha dettagliato come certe minoranze etniche siano soggette a

³ Immaginari sociotecnici che si sono lentamente sviluppati, nel corso degli anni, tramite relazioni dialogiche tra promotori e critici dell'uso di strumenti di IA, e che hanno portato alla creazione di una mitologia dell'IA dall'ampio impatto culturale (S. Natale, A. Ballatore, 2020).

tassi più elevati di forme di sorveglianza da parte delle forze di polizia nelle zone in cui vivono. È questa una dinamica spesso innescata da algoritmi di polizia predittiva che vengono formati su dati pre-esistenti (es., il numero di arresti in un determinato quartiere) ma che possono risultare distorti dal punto di vista etnico a causa di problemi sociali strutturali e situazionali (si veda, a titolo esemplificativo, B.E. Harcourt, 2015; J. Angwin, J. Larson, 2016; A. Ferguson, 2017); una concentrazione di maggiori controlli porta, ovviamente, ad un aumento di segnalazioni ancora maggiore, dando vita a un circolo vizioso di dati che si autoalimentano (un fenomeno generalmente codificato come “discriminazione algoritmica” – M. Barbera, 2021; P. Dunn, 2022)⁴. Più generalmente, le capacità decisionali e predittive degli algoritmi vengono criticate in quanto facilmente, direttamente o indirettamente, vittime di *bias* (errori), andando a inficiare l’equità del risultato finale (P.B. de Laat, 2017; S. Silva, M. Kennedy, 2017). La problematica è rilevante a tal punto che, laddove sistemi di *smart policing* sono stati sperimentati o implementati da qualche anno (come nel Regno Unito per quanto attiene l’utilizzo di software per determinare aree urbane “a rischio”, o l’utilizzo di tecnologia di riconoscimento facciale), vi è una certa resistenza da parte delle Forze dell’ordine nell’utilizzarli, in difesa della propria “agentività” (A. Sandhu, P. Fussey, 2020), o tali sistemi sono stati fortemente criticati da analisi indipendenti (P. Fussey, D. Murray, 2019). Indubbiamente, l’evidenza empirica circa la possibilità reale di contenere episodi criminali, o minimizzare i loro danni, a partire da tecnologie di AI resta al momento limitata (A.J. Meijer, M. Wessels, 2019; S. Tulumello, F. Iapaolo, 2021).

Per quanto riguarda la trattazione di elementi di criticità in ambito di *smart policing*, va inoltre menzionata la letteratura che si è occupata del suo confronto con le normative esistenti e, in particolare, in ambito italiano, con il Regolamento Europeo sulla Protezione dei dati (GDPR). Comprensibilmente, infatti, a seguito dell’entrata in vigore del GDPR sono emersi profili di interesse in relazione alla protezione dei dati personali (A. Bonfanti, 2018; E. Charalambous *et al.*, 2019; P. Perri, 2020). Questo non sorprende, in quanto il GDPR è stata la prima normativa europea ad avere un grande impatto sul digitale, diversamente da precedenti direttive demandate all’implementazione particolare degli Stati, e si anticipa che ulteriori sviluppi si avranno nei

⁴ Un circolo vizioso che, ovviamente, non parte con i modelli di IA. Difatti, l’alterazione negligente o colposa dei tassi di sorveglianza su certi gruppi sociali (in particolar modo minoranze etniche, ma anche ad esempio fasce giovani della popolazione) trae origine da quei processi di *labelling* e stigmatizzazione che sono stati a lungo studiati in criminologia e sociologia della devianza (E. Lemert, 1951; H. Becker, 1963), con la costruzione sociale di ‘popolazioni sospette’ (P. Quinton *et al.*, 2000).

prossimi anni all'entrata in vigore di una serie di normative di rilievo (si veda ad esempio A. Lavorgna, G. Suffia, 2021, in commento alla nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale).

Nella dimensione del rapporto tra lo *smart policing* e la protezione dei dati personali sono rilevanti tutti gli obblighi posti in essere dal GDPR, che prevede la *privacy by design* e *by default* (art. 25) come punto di partenza per immaginare una raccolta di dati e un utilizzo degli stessi all'interno della nostra società europea. Il punto è rilevante non solo poiché qualsiasi tipo di raccolta e trattamento dei dati a fini di *smart policing* deve essere fatto in modo anonimo o pseudonimizzato, ma tendenzialmente poiché si dovrebbe escludere di default qualsiasi raccolta e trattamento di dati personali laddove ciò non sia esclusivamente necessario. Ne consegue la possibilità che molte delle applicazioni dello *smart policing* possano essere considerate contrarie a questo principio, laddove finalizzate a raggiungere un risultato possibile anche senza il trattamento dei dati personali. Tale protezione è accordata in ragione del fatto che, come si è accennato, molto spesso i dati personali utilizzati per inferire caratteristiche come la pericolosità sociale, o la recidiva, possono costituire elementi di discriminazione per individui o gruppi. Una delle tecnologie che risente maggiormente del problema è il riconoscimento facciale, attualmente in fase di ripensamento e limitazione da parte di alcune aziende private finora pioniere del settore, come Facebook e IBM. A tal riguardo si sono pronunciate anche diverse autorità nazionali, come anche il Garante per la protezione dei dati personali italiano in riferimento al software SARI (Sistema Automatico Riconoscimento Immagini) in uso alla Polizia italiana (GPDP, 2021).

Del resto, va notato come, anche a fronte di un'efficacia elevata del sistema, lavorando su grandi numeri ogni margine di errore può ricadere su migliaia di persone, creando inefficienze e oneri aggiuntivi per il personale di polizia (si pensi al fermo e all'identificazione non necessari di centinaia di persone, individuate dal sistema, ma poi verificatisi "falsi positivi"). Tale caratteristica è connaturata allo sviluppo stesso di software di questo tipo, chiamati ad operare su grandissimi numeri sia per migliorarsi tramite sistemi di IA, sia per superare alcuni *bias* del proprio funzionamento.

3.3. Il nostro contributo

Come anticipato, il nostro contributo intende "fare luce" su come, nel contesto mediatico italiano, sia stata presentata al grande pubblico la citata tensione tra i due immaginari sociotecnici presentati poc'anzi, quando si parla di datificazione in ambito di sicurezza. Abbiamo deciso di focalizzarci sullo *smart policing* in quanto questo è il settore che ha ottenuto generalmente più

attenzione anche nel mondo della ricerca⁵. Dopo una breve presentazione della metodologia utilizzata per l'analisi mediatica, l'articolo prosegue con l'analisi descrittiva degli articoli e la discussione dei risultati. Da ultimo, sono delineate alcune conclusioni e tracciate indicazioni di ricerca che potranno essere utili per lo studio del tema non solo nel contesto italiano.

4. Metodologia

Gli articoli sono stati individuati tramite l'aggregatore di contenuti Nexis, un software che permette, tra le altre cose, l'accesso a testo piano a una serie di quotidiani italiani tramite una ricerca per parole chiave. Abbiamo limitato la ricerca alle "notizie" (*news*, escludendo ad esempio blog e comunicati stampa) pubblicate in italiano dal 2009 (*i.e.*, il primo anno apparso nei nostri risultati di ricerca) fino alla fine di settembre 2021. Tra i giornali indicizzati da Nexis vi sono sia giornali a tiratura nazionale, sia pubblicazioni a carattere locale o regionale. Abbiamo deciso di focalizzarci solo sulle notizie pubblicate sul "Corriere della Sera", in quanto è il primo quotidiano italiano sia per diffusione che per lettorato (ADS, 2021), comprendendo gli articoli eventualmente pubblicati solo sulle testate regionali dello stesso o negli inserti. Usando la sintassi (smart and polizia) OR (polizia and predittiva) OR ("intelligenza artificiale" and polizia) OR "smart policing" OR "polizia intelligente" OR (predire and crimin*) OR (predire and reat*) OR "riconoscimento facciale" OR (polizia and biometric*), (perfezionata dopo una serie di tentativi di ricerca manuale) abbiamo ottenuto 820 notizie (escludendo i duplicati), che poi sono state "ripulite" manualmente per eliminare ulteriori duplicati o notizie irrilevanti per lo scopo del nostro lavoro (ad esempio, "smart" appariva in molte notizie come modello di automobile, o il riconoscimento facciale era a volte riferito alla funzionalità propria di alcuni telefoni, automobili o altre apparecchiature, ma veniva discusso con mere finalità pubblicitarie). Alla fine del procedimento, 165 notizie sono state mantenute per l'analisi.

L'analisi (del contenuto, qualitativa) si è svolta tramite il supporto del software NVivo per organizzare in maniera sistematica e strutturata i contenuti manifesti e latenti di nostro interesse, secondo il seguente schema di codifica (ulteriormente specificato nella sezione successiva, dove anche il numero dei riferimenti codificati è riportato in parentesi): anno della notizia; luogo di

⁵ Come evidenziato recentemente in A. Lavorgna, P. Ugwuide (2021) in uno studio che ha analizzato gli abstract degli articoli di ricerca pubblicati sull'utilizzo di approcci di IA in ambito di sicurezza e giustizia criminale dal 2009 al 2019. Dallo studio, infatti, emerge come ben oltre la metà delle ricerche sul tema si siano focalizzate sullo *smart policing*.

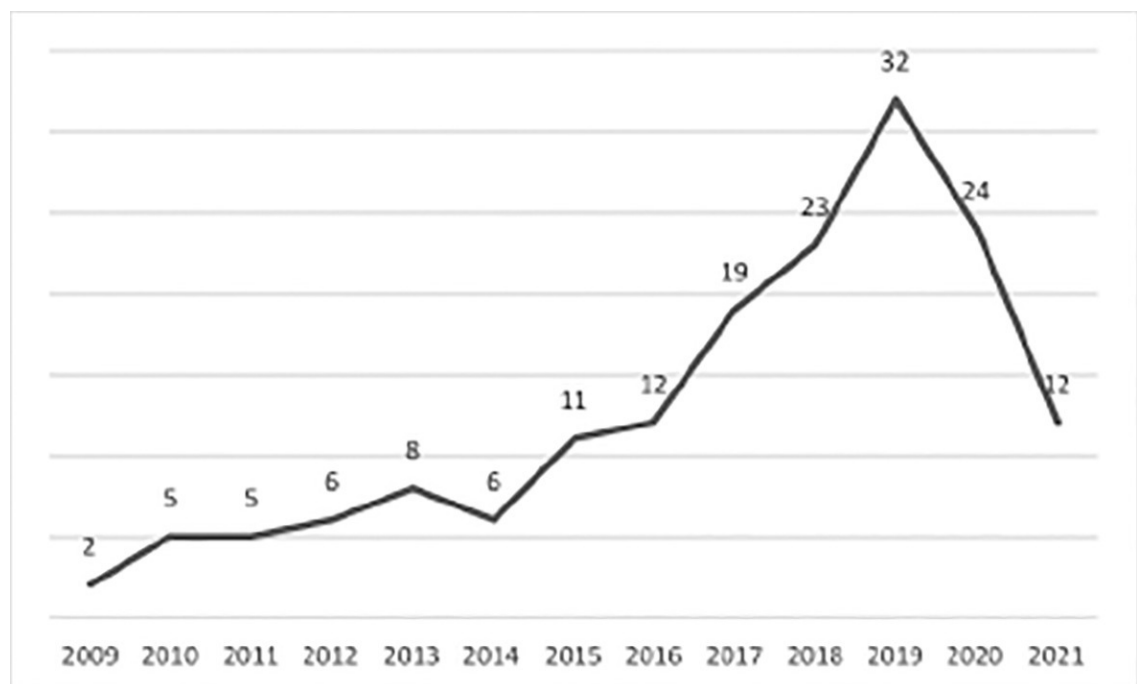
utilizzo; ambiente di utilizzo; settore di utilizzo; ambito di utilizzo; disponibilità della tecnologia descritta; provenienza dei dati utilizzati; narrativa prevalente; riferimenti culturali; riferimenti a ricerche specifiche sul tema.

5. Analisi e discussione

5.1. Il quando e il dove dello *smart policing* nella rappresentazione mediatica

Come emerge chiaramente dalla figura 1, dove i numeri riferiti all'asse delle ordinate indicano il numero di articoli presenti nel nostro database in un dato anno, l'attenzione al tema dello *smart policing* ha avuto una crescita costante nella rappresentazione mediatica studiata, seppur con un leggero calo nell'ultimo biennio – certamente un biennio atipico, considerando la situazione pandemica e i suoi effetti (nelle priorità della copertura mediatica, così come in ambito di percezione di insicurezza e di gestione dei rischi). Questa crescita di attenzione è perfettamente in linea con l'aumento di studi accademici sul tema che è stato osservato nel medesimo arco temporale (A. Lavorgna, P. Ugwu-dike 2021), e conferma la rilevanza contemporanea del tema, sia in ambito specialistico che nella stampa generalista.

Figura 1. Distribuzione per anno



Per quanto riguarda il luogo di utilizzo (tabella 1), l'attenzione dei media si è rivolta principalmente al territorio nazionale (78), con una spiccata attenzione per la Lombardia, seguita da Lazio e Piemonte; molte notizie (56) hanno interessato manifestazioni estere del fenomeno, con particolare attenzione agli Stati Uniti, mentre attenzione a politiche sul tema da parte dell'Unione Europea è stata tutto sommato scarsa (3). Del resto, lo sguardo rivolto verso "l'America" non è elemento di novità nei media italiani, e nel loro ruolo di formazione della cultura e degli immaginari popolari, anche se l'immagine rappresentata è spesso artefatta, immaginaria (E. Scarpellini, J.T. Schnapp, 2012). Va altresì rilevato che la maggior parte delle notizie riguardavano episodi o esempi riferiti a specifiche città, anche se, poi, la narrazione mediatica è sembrata suggerire che alcune tecnologie venissero utilizzate, nel caso di Paesi esteri, in maniera diffusa. In un numero non indifferente di casi (39), comunque, il luogo di utilizzo non è stato specificato: il dato sorprende, se consideriamo che stiamo parlando di tecnologie e di pratiche investigative che sono fortemente dipendenti dal contesto sociale nel quale si sviluppano e vengono utilizzate. Tale assenza di contesto può apparire funzionale alla costruzione di un *sentiment* attorno alle evoluzioni tecnologiche, sia in senso positivo, sia in senso negativo, a prescindere dal dato empirico.

Tabella 1. Luogo di utilizzo

Italia	Lombardia (32); Lazio (10); Piemonte (10); Emilia Romagna (2); Puglia (2); Friuli V.G. (1); Italia in generale (21)
Estero	Stati Uniti (25); Cina (6); Regno Unito (5); Francia (4); Afghanistan (1); Australia (1); Canada (1); Corea del Sud (1); Dubai (1); Germania (2); Giappone (1); India (1); Israele-Palestina (1); Paesi Bassi (1); Russia (1); Serbia (1); Taiwan (1)
Unione Europea	(3)
Non specificato	(39)

È risultato inoltre evidente come il cosiddetto "ambiente urbano" sia quello maggiormente interessato dallo *smart policing*, pur in presenza di scenari, come i confini e le aree periferiche, in cui il controllo attraverso nuove tecnologie potrebbe trovare ampie applicazioni. Per quanto riguarda gli ambienti di utilizzo, infatti, lo spazio specifico della città ha raccolto il maggior numero di riferimenti (con 36 notizie facenti riferimento, in generale, alle città), seguito da stadi (20, con riferimento sia alla digitalizzazione degli accessi, sia

al rilevamento di cori razzisti – il calcio, in Italia, si conferma come uno degli argomenti più mediatici), aeroporti (16) e abitazioni private (10). Seguono riferimenti alla mobilità e trasporti (9), negozi e centri commerciali (5), scuola e istruzione (4), tribunali o studi legali (4), carceri (3), ospedali e sanità (2), intrattenimento e spettacoli (2), luoghi di culto (1) e infine un riferimento a luoghi di lavoro in generale (1). Va, comunque, rilevato come l'ambito di utilizzo non sia stato specificato in un numero considerevole di notizie (65), confermando come la rappresentazione mediatica dello *smart policing* tenda a volte a muoversi su un piano quasi immaginario, e difetti di riportare puntualmente esempi concreti, precisi, dell'utilizzo di certe tecnologie, o una loro disamina critica.

Interessante è anche l'ambito di utilizzo dello *smart policing* nella rappresentazione mediatica analizzata, in cui spicca l'attenzione alla sicurezza urbana (generalmente in un'ottica di prevenzione anticrimine, 69) e al terrorismo (37, specialmente negli articoli più datati), e più in generale al lavoro della polizia giudiziaria (generalmente a scopo di indagine post-segnalazione di reato, 47), seguiti da una relativa attenzione ai procedimenti di digitalizzazione della pubblica amministrazione (28), strumento spesso necessario in un contesto di datificazione. Seguono gli ambiti della sicurezza personale (21), della prevenzione dei furti in abitazioni private o in attività commerciali (13), della sicurezza informatica generalmente intesa (11), nonché della tutela dei minori online (4) e di supporto ad attività di attivismo digitale (3). Abbiamo inoltre individuato discussioni legate a questioni di *social scoring* (6), all'implementazione di misure di salute pubblica nel contesto del Covid-19 (5), e di realtà aumentata (3). In generale, applicazioni nell'ambito del settore pubblico (114) hanno ricevuto più referenze, e quindi più attenzione, rispetto ad applicazioni nel settore privato (59) – un dato che non sorprende considerando che la maggior parte degli articoli fanno riferimento a un contesto, quello italiano, non particolarmente privatizzatore nell'ambito della sicurezza (F. Battistelli, 2013).

5.2. Il cosa e il come dello *smart policing* nella rappresentazione mediatica

La letteratura sul tema ha già discusso come spesso, quando si discute dei pregi delle tecnologie *smart* e del loro utilizzo in ambiti delicati come quello della giustizia penale, si faccia spesso riferimento a tecnologie in studio o potenziali e ai loro sviluppi futuri – anche se spesso queste vengono pubblicizzate come pronte all'uso –, mentre le loro applicazioni in uso correntemente siano spesso soggette ad aspre critiche. Nella loro analisi delle pubblicazioni accademiche sul tema, ad esempio, A. Lavorgna e P. Ugwu-dike (2021) rilevano come più della metà degli studi pubblicati faccia riferimento a tecnologie

non ancora esistenti. Questa confusione, o perlomeno mancanza di precisione, è stata ritrovata anche nell'analisi mediatica effettuata: dal tenore di molti articoli analizzati (125) sembrava di avere a che fare con tecnologie e sistemi già in uso, e si rileva solo un numero minore di riferimenti in cui le tecnologie erano chiaramente presentate come ancora in una mera fase di sviluppo o potenziali (46). Successivi approfondimenti hanno, tuttavia, mostrato come nella realtà anche molti dei sistemi presentati come esistenti fossero invece in una fase progettuale-sperimentale, e non di piena utilizzazione. È interessante rilevare, inoltre, come siano state riscontrate solo 5 referenze a ricerche specifiche sul tema, rivelando una non sorprendente disconnessione tra il mondo della stampa generalista italiana e quello della ricerca, specie accademica, sul tema.

Abbiamo discusso precedentemente come il valore delle tecnologie *smart* dipenda direttamente dalla bontà dei dati alla loro base, e dalla possibilità che essi contengano *bias*, omissioni, o eccessive semplificazioni. Per quanto riguarda l'origine dei dati utilizzati nei casi di *smart policing* presentati negli articoli analizzati, i dati biometrici sono prevalenti (129), seguiti da dati rilevati da telecamere a circuito chiuso (78), sensori/microchip (inclusi gli assistenti vocali) (29), *control room* e sistemi evoluti in uso alle polizie (e.g., il SARI, 23), dati forniti da utenti come nel caso dei dati dei *social media* (16), o dati investigativi (13). Dati amministrativi (6), giudiziari (2) e registri, elenchi pubblici e *open data* (2) vengono menzionati molto più raramente, nonostante abbiano nella pratica operativa un ruolo centrale (L. Bennet Moses, J. Chan, 2018; K. Hannah-Moffat, 2018).

Al di là della panoramica descrittiva presentata nella sezione e nei paragrafi precedenti, è di particolare interesse vedere quali sono le narrative utilizzate nel linguaggio mediatico nel rappresentare lo *smart policing*, in quanto queste sono legate a doppio filo alla sua percezione da parte della cittadinanza e dei decisori politici. L'analisi delle notizie del *Corriere* analizzate ha dapprima individuato quattro categorie narrative principali, all'interno delle quali abbiamo individuato delle tematiche ricorrenti. Nel complesso, la maggior parte delle notizie hanno dipinto lo *smart policing*, nelle sue varie forme, in modo positivo (87); seguono notizie di stampo neutrale o meramente informativo (38), notizie con toni chiaramente negativi (29), e infine notizie che presentano una posizione più articolata (11).

Le narrative di tipo neutrale/informativo sono state generalmente riscontrate in articoli brevi, spesso inferiori alle 500 parole, che si limitavano ad un unico dato fattuale. Vi erano, ad esempio, comunicati stampa, annunci di nuove implementazioni, brevi documentazioni di episodi specifici. Da questa tipologia di articoli non è stato possibile rinvenire alcuna connotazione positiva o negativa, come invece negli articoli di seguito analizzati.

Le narrative positive sono accomunate dalla presenza di immaginari sociotecnici di tipo utopistico, in cui le innovazioni tecno-scientifiche sono benvenute in quanto migliorative della società (S. Jasanoff *et al.*, 2007). Alcune tecnologie, come ad esempio il riconoscimento facciale (fin dalla prima comparsa, in occasione della cattura e del riconoscimento di Osama Bin Laden), sono presentate come realtà in procinto di cambiare per sempre alcuni dei modi fondamentali di gestione della società, in rapporto al crimine e alla sicurezza. Altri riferimenti alle “applicazioni più interessanti”, o “all’avanguardia”, lasciano intendere che l’evoluzione naturale di molti progetti sia la larga applicazione su scala nazionale e globale, creando aspettative potenzialmente distorte nei lettori (in linea con quanto osservato internazionalmente nell’analisi mediatica di altre storie di techno-ottimismo, ad esempio in Giappone – S. Asayama, A. Ishii, 2017 – o in Germania – L. Jelinski *et al.*, 2021). Tale visione è indicativa della difficoltà di cogliere, sul momento, quali applicazioni o tecnologie siano realmente in grado di segnare un passaggio rilevante, o siano piuttosto destinate ad una rapida obsolescenza. Di ciò è certamente responsabile l’avanzamento tecnologico accelerato cui stiamo assistendo, e che ha caratterizzato il decennio 2010-2020, così come la portata globale di casi e applicazioni, che certamente aumenta il numero di eventi notiziabili e da registrare come possibili innovazioni.

Nella limitata lunghezza propria degli articoli di stampa, la positività delle applicazioni di *smart policing* è risultata presentata in differenti modi, tra cui si segnalano: l’obiettività scientifica (le tecnologie utilizzate sono descritte come scientifiche e capaci di minimizzare la fallibilità intrinseca nella natura umana; conseguentemente, da un punto di vista sociale, l’utilizzo della tecnologia è visto come auspicabile); la superiorità tecnologica (la competenza della tecnologia utilizzata viene presentata come superiore a quella umana in termini di efficacia ed efficienza); l’utilità vitale (la tecnologia è presentata come critica, essenziale per questioni di pubblica sicurezza, ad esempio per quanto riguarda l’allocazione efficiente delle scarse risorse a disposizione, e il miglioramento della percezione circa la legittimità delle forze di polizia), e la cosiddetta usabilità (*usability*)⁶. Le tecnologie alla base dello *smart policing* sono generalmente descritte come semplici da usare, alla portata di tutti, o persino risolutive di problemi pratici. La facilità di utilizzo è presentata sia che si tratti di utilizzare tecnologie complesse per sbloccare dispositivi per-

⁶ La concettualizzazione utilizzata si basa su quella proposta nell’analisi di A. Lavorgna e P. Ugwu-dike (2021) nell’identificare le cornici narrative positive utilizzate in articoli accademici. Si può dunque rilevare la convergenza di tali narrative sia in pubblicazioni specialistiche (specialmente in ambito informatico) che mediatico.

sonali, sia per gestire intere città. Si sottintende, o trascura, la necessità di un'adeguata formazione del personale addetto all'utilizzo.

Un ulteriore rafforzamento della narrazione positiva è riscontrabile nei casi di sistemi di *smart policing* sviluppati da privati, in uso o con destinazione pubblica. L'effettiva descrizione del sistema viene sovente operata solo dal produttore, unico a conoscere il funzionamento di un sistema in via di attivazione. Tali descrizioni non sono state generalmente verificate da studi indipendenti, volti a comprovare o smentire la correttezza delle dichiarazioni ufficiali. Sono poi rarissimi i casi in cui tali sistemi siano stati oggetto di cronaca sul loro effettivo "successo" dopo un ragionevole periodo di utilizzo. Il mantenimento delle promesse iniziali, pertanto, risulta generalmente non documentato, né a livello mediatico, né a livello scientifico. Questo problema è legato a una questione ampiamente discussa in letteratura negli ultimi anni, ossia il rapporto tra capitale sociale/critico/intellettuale (con ovvi riferimenti a P. Bourdieu, 1986) e capitale digitale (la capacità di accedere a e capitalizzare le risorse legate alle tecnologie digitali, si veda J. Van Dijk, 2005). Non solo i detentori del cosiddetto capitale digitale (ad esempio produttori e sviluppatori, e più in generale informatici e *data scientist*, che nel complesso vanno a formare una "rete tecnoepistemica" di esperti – si veda I.F. Ballo, 2015, 10) possono dominare le scelte architettoniche delle nuove tecnologie, quindi influenzandone direttamente i risultati algoritmici e risultandone meno danneggiati, ma essi (generalmente privati) possono anche influenzarne le narrative, anche laddove tali tecnologie vadano a intrecciarsi con funzioni primarie dello Stato (P.R. Blair *et al.*, 2008; A. Završnik, 2021; A. Lavgorgna, P. Ugwudike, 2021).

Si è rilevato inoltre come la rappresentazione delle tecnologie di *smart policing* sia generalmente priva di riferimenti precisi allo stato dell'arte della materia, e dei riferimenti necessari per una visione d'insieme del tema. Oltre al citato caso dei progetti implementati in una specifica realtà, o in contesti geografici estremamente circoscritti (*e.g.*, una singola città), si registrano numerosi casi in cui lo *smart policing* è presentato come unicamente mosso da ragioni di efficienza per l'utente-consumatore. È il caso degli aeroporti, per i quali la digitalizzazione delle procedure di check-in è stata generalmente presentata slegata da ragioni di sicurezza e di gestione di un volume di informazioni sempre più ingente, ragioni che pure sono alla base della lunghezza delle procedure.

Nel caso di narrative negative, si è trattato perlopiù di articoli in cui, da un lato, si evidenziavano le inefficienze e le limitazioni tecniche dei sistemi di *smart policing* (ad esempio, poiché non in grado di rispondere alle aspettative sul loro utilizzo, in linea con la concettualizzazione del "tecno-sciovinismo" proposta a M. Broussard, 2018, nella loro critica all'efficienza e alla neutra-

lità scientifica delle tecnologie *smart*), o si registravano limitazioni di natura giuridica all'utilizzo. Tra queste ultime, le principali sono state per violazioni di privacy (tra le maggiori, anche in relazione all'entrata in vigore del GDPR nel 2016 – si veda sezione 3.2) e per il pericolo di discriminazione (ad esempio, nel caso di un cittadino afroamericano “arrestato nel giugno 2020 per un crimine che non aveva commesso solo perché la polizia si era affidata in modo acritico al responso di un sistema di riconoscimento facciale”). In un numero minore di casi si è evidenziata l'opacità algoritmica o la regolamentazione inadeguata.

Infine, le narrative che presentano una posizione più articolata rimandano alle tematiche cosiddette ambivalenti o soluzioniste (per riprendere, anche in questo caso, la concettualizzazione proposta in A. Lavorgna, P. Ugwu-dike, 2021). Nella nostra analisi mediatica, queste narrative solitamente sono state riscontrate in articoli più lunghi e complessi, affidati talvolta a autori noti o percepiti come autorevoli a livello nazionale in pezzi d'opinione. Nel complesso, in questi articoli emerge una posizione più equilibrata, che sottolinea sia il potenziale che i limiti di certe tecnologie *smart*. In alcuni articoli si è fatto riferimento alla cosiddetta “realtà diminuita”, ovvero alla possibilità di rimuovere deliberatamente parti dello scenario del mondo reale o rimpiazzarle con contenuti generati al computer, S. Mann, B. Woodrow, 2003). La rilevanza e la pervasività dell'alterazione del reale, con tecnologie che possono essere utilizzate per nascondere situazioni di criticità e di disagio sociale, non ha tuttavia trovato spazio in anni più recenti, travolta dalla crescente datificazione che, apparentemente, coinvolge ogni aspetto e ambito dell'attività umana. Talvolta si sono presentati risultati scientifici relativi all'efficacia delle misure adottate. In molti casi, nonostante un apprezzamento in generale della tecnologia in questione, viene criticato il suo utilizzo in un ambito specifico; le motivazioni sono legate al rischio di generare un potenziale danno sociale, come la discriminazione di gruppi o la violazione di diritti collettivi e individuali. Ne è derivata una posizione certamente più articolata, meno enfatica e meno sensazionalistica, maggiormente orientata alla ricerca del compromesso necessario tra digitalizzazione e tutele.

Prima di concludere, è interessante notare come nelle rappresentazioni mediatiche siano presenti una serie di riferimenti culturali e popolari, anche questi rilevanti in un'ottica di criminologia culturale in quanto mediazioni (narrative, visive, cinematografiche) che contribuiscono a generare immaginari sociali (K.J. Hayward, J. Young, 2004). Il caso più frequente – e questo certo non sorprende – è legato a *Minority Report* (11), il film del 2002 diretto da Steven Spielberg e ispirato dall'omonimo racconto di fantascienza di Philip K. Dick. In esso la polizia riesce a impedire gli omicidi prima che questi avvengano e ad arrestare i potenziali colpevoli grazie a un sistema chiamato

“Precrime”. Il riferimento al film, per quanto evocativo di una visione distopica del futuro tecnologico, resta tuttavia superficiale: la rappresentazione mediatica sembra limitarsi a richiamare un immaginario in cui dati biometrici sono usati a scopo predittivo in una sorta di determinismo sociale, glissando su come, nel film, l’infallibilità algoritmica venga invece riconosciuta, così come l’incapacità degli algoritmi di analizzare la totale complessità dell’azione umana e sociale. Tra gli altri rimandi ad una società della predizione (e ai problemi etici che questa comporta) si sono rilevati *1984* di Orwell (1), e il film *La zona morta* (1). Il riferimento al film *2001 Odissea nello Spazio* (1) è interessante nel suggerire i rischi di una tecnologia che possa prendere il controllo sull’“agentività” umana. Particolarmente “mediatico” è invece il riferimento a *Robocop* (1) in una notizia facente riferimento all’utilizzo, in un paese estero, di un poliziotto-robot: anche se in grado di leggere le espressioni facciali di una persona e reagire in sei lingue, in maniera autonoma, il sistema appare alquanto limitato e non equiparabile in pratica ad un vero agente di polizia. Una trattazione delle rappresentazioni cinematografiche dello *smart policing* esula dallo scopo di questo studio esplorativo; un’analisi approfondita di come tali rappresentazioni siano cambiate nel tempo e di come abbiano forgiato gli immaginari sociotecnici in materia viene auspicata.

6. Note conclusive e nuove prospettive di ricerca

Dall’analisi proposta emerge come ci sia una insufficiente consapevolezza e capacità critica in merito alle nuove tecnologie e al loro utilizzo, legata a una tendenza all’eccessiva sicurezza nei confronti della fonte d’origine dell’informazione. Alcune considerazioni, di ordine più generale, possono essere condotte circa l’adeguatezza delle nostre definizioni e categorie per descrivere la datificazione in atto in ogni ambito della vita umana e, in particolare, in ogni fenomeno sociale. Vi è il sospetto che, talvolta, dietro alle formule più utilizzate – e ripetute – vi sia una generica allusione a temi e ambiti che si suppone conosciuti da parte del lettore, piuttosto che una precisa definizione di quali essi siano. È certamente il caso del termine “smart”, utilizzato per indicare ambiti relativi alla datificazione digitale. Il termine vorrebbe concentrare l’attenzione sull’aspetto tecnico, non precisando alcuna finalità di utilizzo (a differenza, ad esempio, di termini come “predictive”). Tuttavia, esso non è un termine neutro. Nell’uso comune, infatti, suggerisce l’adozione di una tecnologia migliorativa, generalmente in grado di prendere decisioni “intelligenti”. Più verosimilmente, invece, il termine “smart” dovrebbe indicare strumenti in grado di agire secondo le istruzioni fornite.

L’assenza dell’approfondimento giornalistico, spesso parallelamente a quello scientifico, è dovuta alla non adeguata conoscenza di come tali sistemi

operino e in base a quali meccaniche e presupposti. Alla luce di questo, è quanto mai necessario andare a investigare, a livello di cronaca, entrambe le facce della tecnologia, che sono sia positive che negative, funzionanti o non funzionanti. Per fare ciò, si suggerisce l'elaborazione di nuove linee guida per il giornalismo sul come inquisire il rapporto tra le nuove tecnologie e la realtà sociale. In particolare, sarebbe di giovamento includere il punto di vista socio-criminologico, senza tralasciare l'aspetto tecnico, nel riportare mediaticamente casi e applicazioni di sistemi di *smart policing*, in modo da riequilibrare, almeno in parte, lo sbilanciamento anche mediatico tra quel capitale sociale/critico/intellettuale e il capitale digitale discussi precedentemente. Del resto, va tenuto a mente che, tra i riceventi dell'informazione di un quotidiano generalista vi sono anche quei responsabili politici, forze dell'ordine e altri professionisti che potrebbero utilizzare o fare affidamento sulle tecnologie o i sistemi descritti, ma che molto spesso non hanno sufficiente capitale né critico né digitale (L. Sanchez *et al.*, 2019) per comprenderne appieno anche i limiti.

Più in generale, auspichiamo che l'analisi mediatica esplorativa qua presentata, la trattazione dei diversi immaginari sociotecnici e la presentazione della letteratura critica, specialmente socio-criminologica e di natura internazionale, che negli ultimi anni è stata prodotta sul tema possano essere di spunto ai colleghi che si occupano di sicurezza nelle sue numerose implicazioni, sia da un punto di vista teorico che operativo. Riteniamo infatti che le sfide poste dalla datificazione al giorno d'oggi non possano essere ignorate da chi, per formazione, inclinazione o funzione, si occupa a vario titolo di giustizia, criminalità e devianza, o di politiche e responsabilità sociali, considerando certamente le possibilità offerte dai sistemi *smart* al centro del nostro contributo, ma anche i potenziali danni sociali ad essi ormai ampiamente associati.

Riferimenti bibliografici

- ADS (2021), *Accreditamenti Diffusione Stampa*, in <https://www.adsnotizie.it/>.
- ANGWIN Julia, LARSON Jeff (2016), *Bias in criminal risk scores is mathematically inevitable, researchers say*, in <https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say>.
- ASAYAMA Shinichiro, ISHII Asayama (2017), *Selling stories of techno-optimism? The role of narratives on discursive construction of carbon capture and storage in the Japanese media*, in "Energy research & social science", 31, pp. 50-59.
- BAACK Stefan (2015), *Datafication and empowerment: How the open data movement rearticulates notions of democracy, participation and journalism*, in "Big Data & Society", 7, 1.
- BALLO Ingrid Foss (2015), *Imagining energy futures: Sociotechnical imaginaries of the future smart grid in Norway*, in "Energy Research & Social Science", 9, pp. 9-20.

- BARBERA Marzia (2021), *Discriminazioni algoritmiche e forme di discriminazione*, in "Labour & Law Issues", 7, 1.
- BAROCAS Solon, SELBST Andrew D. (2016), *Big data's disparate impact*, in "California Law Review", 104, pp. 671-732.
- BASILE Fabio (2019), *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in "Diritto Penale & Uomo", in <https://www.penalecontemporaneo.it/upload/3089-basile2019.pdf>.
- BATTISTELLI Fabrizio (2013), *Sicurezza urbana "partecipata": privatizzata, statalizzata o pubblica?*, in "Quaderni di Sociologia", 63, pp. 105-126.
- BECKER Howard S. (1963), *Outsiders: Studies in the sociology of deviance*, The Free Press, New York.
- BENBOUZID Bilel (2019), *To predict and to manage. Predictive policing in the United States*, Big Data & Society.
- BENNETT Tony, CURRAN James, GUREVITCH Michael, WOOLLACOTT Janet, a cura di (1982), *Culture, society and the media*, Methuen, London.
- BENNETT MOSES Lyria, CHAN Janet (2018), *Algorithmic prediction in policing: Assumptions, evaluations, and accountability*, in "Policing and Society", 28, 7, pp. 806-822.
- BIBRI Simon Elias (2019), *Advances in smart sustainable urbanism: Data-driven and data-intensive scientific approaches to wicked problems*, Proceedings of the 4th International Conference on Smart City Applications.
- BLAIR Pamela R., MARCUS David K., BOCCACCINI Marcus T. (2008), *Is there an allegiance effect for assessment instruments? Actuarial risk assessment as an exemplar*, in "Clinical Psychology: Science and Practice", 15, 4, pp. 346-360.
- BONFANTI Angelica (2018), *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in "Media Laws", 3, pp. 1-13.
- BORGHI Maurizio (2018), *Data portability and regulation of digital markets*, in "Mercato Concorrenza Regole", 2, pp. 223-247.
- BOURDIEU Pierre (1986), *The forms of capital*, in John G. RICHARDSON, a cura di, *Handbook of theory and research for the sociology of education*, Greenwood Press, Westport, pp. 241-258.
- BOYD Danah, CRAWFORD Kate (2012), *Critical questions for big data*, in "Information, Communication & Society", 15, 5, pp. 662-679.
- BRAYNE Sarah (2017), *Big data surveillance: The case of policing*, in "American Sociological Review", 82, 5, pp. 977-1008.
- BROUSSARD Meredith (2018), *Artificial unintelligence: How computers misunderstand the world*, The MIT Press, Cambridge.
- BROWNSWORD Roger, HAREL Alon (2019), *Law, liberty and technology: Criminal justice in the context of smart machines*, in "International Journal of Law in Context", 15, 2, pp. 107-125.
- BURNEY Elizabeth (2009), *Making people behave: Anti-social behaviour, politics and policy*, Routledge, London.
- CAMACHO-COLLADOS Miguel, LIBERATORE Federico (2015), *A decision support system for predictive police patrolling*, in "Decis. Support Syst.", 75, pp. 25-37.
- CHAN Janet, BENNETT MOSES Lyria (2017), *Making sense of big data for security*, in "British Journal of Criminology", 57, pp. 299-319.

- CHARALAMBOUS Elisavet, SKITSAS Michael, EFSTATHIOU Nectarious, KOUTRAS Nikolaos (2019), *A digital decision support system for efficient policing in urban security in a community policing context*, in Georgios LEVENTAKIS, Maria HABERFELD, a cura di, *Synergy of community policing and technology*, SpringerBriefs in Criminology, Springer, Cham, pp. 1-14.
- COHEN Stanley (1972), *Folk devils and moral panics: The creation of the mods and rockers*, Basil, Oxford.
- COLDREN James R., HUNTOON Alissa, MEDARIS Michael (2013), *Introducing smart policing: Foundations, principles, and practice*, in "Police Quarterly", 16, 3, pp. 275-286.
- COLUCCIA Anna, FERRETTI Fabio, LORENZI Lore, BURACCHI Tommaso (2014), *Media e percezione della sicurezza. Analisi e riflessioni*, in "Rassegna Italiana di Criminologia", 2.
- COMMISSIONE EUROPEA (2018), *Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni. L'intelligenza artificiale per l'Europa*, COM(2018), pp. 237.
- CUSTERS Bart H.M. (2013), *Data dilemmas in the information society*, in Bart H.M. CUSTERS, Toon CALDERS, Bart SCHERMER, Tal Z. ZARSKY, a cura di, *Discrimination and privacy in the information society*, Springer, Heidelberg, pp. 3-26.
- DE FRANCESCHI Alberti, LEHMANN Mixhael (2015), *Data as tradable commodity and new measures for their protection*, in "Italian Law Journal", 1, 1, pp. 51-73.
- DE LAAT Paul B. (2017), *Big data and algorithmic decision-making: Can transparency restore accountability?*, in "Acm Sigcas Computers and Society", 47, 3, pp. 39-53.
- DUNN Pietro (2022), *Moderazione automatizzata e discriminazione algoritmica: il caso dell'hate speech*, in "Rivista italiana di informatica e diritto", 4, 1, pp. 12.
- ENSIGN Danielle, FRIEDLER Sorelle A., NEVILLE Scott, SCHEIDEGGER Carlos, VENKATASUBRAMANIAN Suresh (2018), *Runaway feedback loops in predictive policing. Paper presented at the Machine Learning Research*, in "Conference on Fairness, Accountability, and Transparency", 81, pp. 1-12.
- ESPOSITO Elena (2013), *Digital prophecies and web intelligence*, in Mireille HILDEBRANDT, Klaas DE VRIES, a cura di, *Privacy, due process and the computational turn*, Routledge, London, pp. 135-156.
- FERGUSON Andrew G. (2017), *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press, New York.
- FERRELL Jeff (2013), *Cultural criminology and the politics of meaning*, in "Critical Criminology", 21, pp. 257-271.
- FINOCCHIARO Giusella (2019), *Intelligenza artificiale e protezione dei dati personali*, in "Giurisprudenza Italiana".
- FUSSEY Pete, MURRAY Daragh (2019), *Independent report on the London metropolitan police service's trial of live facial recognition technology*, in <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf>.
- GPDP (2021), *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy*, Garante per la Protezione dei Dati Personali, in <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842>.

- GRUETZEMACHER Ross, WHITTLESTONE Jess (2019), *Defining and unpacking transformative AI*, EAG, London.
- HANNAH-MOFFAT Kelly (2018), *Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates*, in "Theoretical Criminology", 23, 4, pp. 453-470.
- HARCOURT Bernard E. (2015), *Risk as a proxy for race*, in "Federal Sentencing Reporter", 27, pp. 237-243.
- HAYWARD Keith J., YOUNG Jock (2004), *Cultural criminology: Some notes on the script*, in "Theoretical Criminology", 8, 3, pp. 259-273.
- HOLLYWOOD John S., WOODS Dulani, LAULAND Andrew, BRIAN A. Jackson, SILBERGLITT Richard (2018), *Emerging technology trends and their impact on criminal justice*, RAND Corporation, Santa Monica.
- ILIADIS Andrew, RUSSO Federica (2016), *Critical data studies: An introduction*, in "Big Data & Society" 3, 2, pp. 1-7.
- JASANOFF Sheila, SANG-HYUN Kim, SPERLING Stefan (2007), *Sociotechnical imaginaries and science and technology policy: A cross-national comparison*, in <https://stsprogram.org/admin/files/imaginaries/NSF-imaginaries-proposal.pdf>.
- JELINSKI Lena, ETZRODT Katrin, ENGESSER Sven (2021), *Undifferentiated optimism and scandalized accidents: The media coverage of autonomous driving in Germany*, in "Journal of Science Communication", 20, 4, A02.
- KAUFMANN Mareile, EGBERT Simon, LEESE Matthias (2019), *Predictive policing and the politics of patterns*, in "The British Journal of Criminology", 59, 3, pp. 674-692.
- LAVORGNA Anita, SUFFIA Gabriele (2021), *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale: un passo necessario, ma non sufficiente, nella giusta direzione*, in "Diritto Penale Contemporaneo", 2, pp. 88-105.
- LAVORGNA Anita, UGWUDIKE Pamela (2021), *The datafication revolution in criminal justice: An empirical exploration of frames portraying data-driven technologies for crime prevention and control*, in "Big Data & Society", 8, 2.
- LAW SOCIETY (2019), *Algorithm use in the criminal justice system report*, in <https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report>.
- LEIGH Johanna, DUNNETT Sarah, JACKSON Lisa (2019), *Predictive police patrolling to target hotspots and cover response demand*, in "Annals of Operations Research", 283, 1, pp. 395-410.
- LEMERT Edwin M. (1951), *Social pathology*, McGraw-Hill, New York.
- LEUZZI Fabio, DEL SIGNORE Emiliano, FERRANTI Rosanna (2018), *Towards a pervasive and predictive traffic police*, in Fabio LEUZZI, Stefano FERILLI, a cura di, *Traffic mining applied to police activities*, TRAP 2017, in "Advances in Intelligent Systems and Computing", vol. 728, Springer, Cham.
- LUM Kristian, ISAAC William (2016), *To predict and serve?*, in "Significance", 13, pp. 14-19.
- MANN Steve, WOODROW Barfield (2003) *Introduction to mediated reality*, in "International Journal of Human – Computer Interaction", 15, 2, pp. 205-208.
- MASTROBUONI Giovanni (2020), *Crime is terribly revealing: Information technology and police productivity*, in "Review of Economic Studies", 87, 6, pp. 2727-2753.

- MCGUIRE Michael (2018), *Beyond flatland: When smart cities make stupid citizens*, in "City, Territory and Architecture", 5, 22.
- MEIJER Albert, WESSELS Martin (2019), *Predictive policing: Review of benefits and drawbacks*, in "International Journal of Public Administration", 42, pp. 1031-1039.
- NATALE Simone, BALLATORE Andrea (2020), *Imagining the thinking machine: Technological myths and the rise of artificial intelligence*, in "Convergence", 26, 1, pp. 3-18.
- NAZIONI UNITE (2014), *World that counts: Mobilising the data revolution for sustainable development*, in <https://www.undatarevolution.org/wpcontent/uploads/2014/12/A-World-That-Counts2.pdf>.
- PERRI Pierluigi (2020), *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè-Francis Lefebvre, Milano.
- QUINTON Paul, BLAND Nick, MILLER Joel (2000), *Police stops, decision-making and practice*, in "Police Research Series Paper", 130, Home Office, London.
- RATCLIFFE Jerry H. (2008), *Knowledge management challenges in the development of intelligence-led policing*, in "The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions", John Wiley and Sons, Chichester, pp. 205-220.
- RATCLIFFE Jerry H. (2016), *Intelligence-led policing*, Routledge, London.
- SANCHEZ Laura, GRAJEDA Cinthya, BAGGILI Ibrahim (2019), *A practitioner survey exploring the value of forensic tools, AI, filtering, & safer presentation for investigating child sexual abuse material (CSAM)*, in "Digital Investigation", 29, pp. 124-142.
- SANDHU Ajay, FUSSEY Peter (2020), *The "uberization of policing"? How police negotiate and operationalise predictive policing technology*, in "Policing and Society", 31, pp. 66-81.
- SCARPELLINI Emanuela, SCHNAPP Jeffrey T., a cura di (2012), *ItaliAmerica: il mondo dei media*, il Saggiatore, Milano.
- SILVA Selena, KENNEY Martin (2018), *Algorithms, platforms, and ethnic bias: An integrative essay*, in "Phylon", 55, 1-2, pp. 9-37.
- SOFIA Cistina (2004), *Analisi del contenuto, comunicazione, media. Evoluzione, applicazioni e tecniche*, Franco Angeli, Milano.
- STARR Sonja B. (2014), *Evidence-based sentencing and the scientific rationalization of discrimination*, in "Stanford Law Review", 66, 4, pp. 803-872.
- SURETTE Ray, KAMPE Kimberly (2016), *The media and criminal justice policy and practices*, in Thomas G. BLOMBERG, Julie M. BRANCALE, Kevin M. BEAVER, William D. BALES, a cura di, *Advancing criminology and criminal justice policy*, Taylor&Francis, London, pp. 428-441.
- TIPALDO Giuseppe (2014), *L'analisi del contenuto e i mass media. Oggetti, metodi e strumenti*, il Mulino, Bologna.
- TONELLO Fabrizio (2008), *La sicurezza nei mass media*, in "Contemporanea", 11, 4, pp. 706-713.
- TULUMELLO Simone, IAPAOLO Fabio (2021), *Policing the future, disrupting urban policy today. Predictive policing, smart city and urban policy in Memphis (TN)*, in "Urban Geography".
- UGWUDIKE Pamela (2020), *Digital prediction technologies in the justice system: The implications of a "race-neutral" agenda*, in "Theoretical Criminology", 24, 39, pp. 482-501.

- VAN DIJK Johannes A.G.M. (2005), *The deepening divide: Inequality in the information society*, Sage, Thousand Oaks.
- WOOD Mark A. (2021), *Rethinking how technologies harm*, in “The British Journal of Criminology”, 61, 3, pp. 627-647.
- ZAVRŠNIK Aleš (2019), *Algorithmic justice: Algorithms and big data in criminal justice settings*, in “European Journal of Criminology”, 18, 4, pp. 623-642.

Abstract

SMART POLICING IN BETWEEN FEARS AND REALITY: AN EXPLORATORY ANALYSIS OF MEDIA REPRESENTATIONS OF SMART POLICING IN ITALY

In our contemporary societies, instances of datafication and smart technologies are increasingly used even in sensitive contexts such as public security and smart policing. While these processes have clear potential, they still suffer from important limitations. This contribution offers an exploratory analysis of how the advent of datafication in the security sector has been portrayed by media in Italy.

Key words: Smart Policing, Media Analysis, Sociotechnical Imaginaries.