CARTOGRAFIE SOCIALI
Rivista di sociologia e scienze umane
Anno IV, n. 8, novembre 2019

Direzione scientifica
Lucio d'Alessandro e Antonello Petrillo

Direttore responsabile
Arturo Lando

Redazione
Elena Cennini, Anna D'Ascenzio, Marco De Biase, Giuseppina Della Sala, Eugenio Galioto, Emilio Gardini, Fabrizio Greco, Luca Manunza

Comitato di redazione
Marco Armiero (KTH Royal Institute of Technology, Stockholm), Tugba Basaran (Kent University), Nick Dines (Middlesex University of London), Stefania Ferraro (Università degli Studi Suor Orsola Benincasa, Napoli), Marcello Maneri (Università di Milano Bicocca), Önder Özhan (Università di Ankara), Domenico Perrotta (Università di Bergamo), Federico Rahola (Università di Genova), Pietro Saitta (Università di Messina), Anna Simone (Università Roma Tre), Ciro Tarantino (Università della Calabria)

Comitato scientifico
Fabienne Brion (Université Catholique de Louvain -la-Neuve), Alessandro Dal Lago (Università di Genova), Davide De Sanctis (Università degli Studi Federico II - Napoli), Didier Fassin (Institute for Advanced Study School of Social Science, Princeton), Fernando Gil Villa (Universidad de Salamanca), Akhil Gupta (University of California), Michalis Lianos (Université de Rouen), Marco Martiniello (University of Liège), Laurent Mucchielli (CNRS - Centre national de la recherche scientifique), Salvatore Palidda (Università di Genova), Michel Peraldi (CADIS - Centre d'analyse et d'intervention sociologiques), Andrea Rea (Université libre de Bruxelles)

"Cartografie sociali" is a peer reviewed journal

TRA POTERE E SAPERE: STUDI CRITICI SULLA VALUTAZIONE

A cura di Davide Borrelli e Diego Giannone

MIMESIS

SUOR ORSOLA UNIVERSITY PRESS

Pubblicazione semestrale: abbonamento annuale (due numeri): € 45,00

Per gli ordini e gli abbonamenti rivolgersi a:
ordini@mimesisedizioni.it
L'acquisto avviene per bonifico intestato a:
MIM Edizioni Srl, Via Monfalcone 17/19
20099 - Sesto San Giovanni (MI)
Unicredit Banca - Milano
IBAN: IT 59 B 02008 01634 000101289368
BIC/SWIFT: UNCRITM1234

Cartografie sociali è una rivista promossa da URiT, Unità di Ricerca sulle Topografie sociali.

Direzione e Redazione della rivista hanno sede
presso l'Università degli Studi Suor Orsola Benincasa
Via Suor Orsola 10 - 80132 Napoli (Italy)
www.unisob.na.it
cartografiesociali@unisob.na.it
cartografiesociali.rivista@gmail.com

UNIVERSITÀ DEGLI STUDI
SUOR ORSOLA
BENINCASA
FACOLTÀ DI
SCIENZE
DELLA FORMAZIONE



MIMESIS EDIZIONI (Milano – Udine)
www.mimesisedizioni.it
mimesis@mimesisedizioni.it

Isbn: 9788857565187
Issn: 2499-7641

© 2019 – MIM EDIZIONI SRL
Via Monfalcone, 17/19 – 20099
Sesto San Giovanni (MI)
Phone: +39 02 24861657 / 24416383
Fax: +39 02 89403935

Registrazione Tribunale di Napoli n. 37 del 5 luglio 2012

INDICE

EDITORIALE: La *neo*valutazione al governo della società
di Davide Borrelli e Diego Giannone *7*

La valutazione: un potere spacciato per sapere
di Yves Charles Zarka 37

Oggetti smarriti e ritrovati. Cartografare i valori politico-morali per comprendere l'ondata della valutazione
di Peter Dahler-Larsen 49

Dal rischio alla prestazione. Dispositivi, misurazioni, produzione del valore e inclusione differenziale
di Anna Simone 71

Il giudizio di Talos. Valutazione, algoritmi, macchine
di Mauro Santaniello 85

Vittime o complici? Sullo strano desiderio di essere valutati
di Bénédicte Vidaillet 103

Measuring and Delimiting Corruption
di Debora Valentina Malito 115

Rating agencies, symbolic capital and the evaluation of nation-states. A preliminary exploration
di Adriano Cozzolino 139

La Repubblica dei *performanti*
ovvero
si hic est asinus non erit illic equus
di Antimo Cesaro 159

The re-emerging debate over the rise of the Evaluative State in the British university sector
di Laura Giovinazzi 185

Recensione a *La mafia dimenticata*
di Salvatore Palidda 199

Mauro Santaniello

IL GIUDIZIO DI TALOS. VALUTAZIONE, ALGORITMI, MACCHINE.

Abstract

Individuals are more and more subjected to evaluation mechanisms managed by algorithmic systems, and a growing universe of human experiences undergo decision-making processes conducted by evaluating assemblages of data and machines. Algorithmic evaluation represents a powerful social mechanism of resource distribution, and one of the most important transformative drivers of contemporary governance systems. The essay provides a definition of algorithmic evaluation, and a brief literature review on its fields of application. Then, the main risks connected to its qualitative and quantitative expansion are investigated through the study of a crucial case with a huge political and social impact: predictive policing. Finally, the paper summarizes the challenges posed by autonomous evaluation systems to contemporary societies, highlighting the gap between, on the one hand, the speed of development and adoption of these new technologies and, on the other hand, the time needed to assess their functioning and effects from a democratic political perspective.

Keywords:

Algorithmic evaluation, Predictive policing, Artificial intelligence, Machine learning

1. *Introduzione*

La diffusione di apparati algoritmici di valutazione che misurano, comparano, classificano, prevedono e decidono in maniera autonoma rappresenta la trasformazione più significativa dei sistemi di governance nel mondo contemporaneo. Tanto nelle democrazie liberali dell'occidente

quanto nei paesi oppressi da regimi autoritari, la valutazione algoritmica va configurandosi come un potente meccanismo sociale di distribuzione delle risorse: dal credito alla carriera, dalle informazioni alle relazioni sociali, dalla reputazione professionale alla fruizione dei servizi pubblici, dalle misure di welfare all'accesso ai mercati nazionali e globali, dalle opportunità commerciali alle possibilità di emigrare, dal godimento delle libertà personali ai diritti politici, civili, economici. Un meccanismo pervasivo, che impatta ambiti sempre più estesi della vita degli individui e dinamiche fondamentali delle società umane.

Sebbene l'utilizzo di algoritmi ai fini della valutazione di processi, prodotti e performance sia una pratica consolidata da tempo in numerosi settori dell'economia, alcuni recenti sviluppi tecno-sociali ne stanno radicalmente trasformando le modalità e gli ambiti di applicazione, amplificandone gli effetti in misura esponenziale. Innanzitutto, la disponibilità di dati ha raggiunto dimensioni senza precedenti nella storia umana. I cosiddetti *big data* sono ormai una realtà sociale ineludibile, prodotta, a sua volta, da almeno tre fattori: i) il regime globale di sostanziale liberalizzazione dell'informazione, che agevola la produzione, la raccolta e lo scambio dei dati; ii) la diffusione di sistemi di datificazione, come l'Internet delle Cose, le Smart City, le tecnologie indossabili, la domotica e la sensoristica, che convertono porzioni crescenti di realtà in informazione digitale; iii) la riduzione drammatica dei costi connessi all'elaborazione, alla trasmissione e all'archiviazione dei dati. In secondo luogo, si assiste di recente a una rapida evoluzione degli stessi algoritmi, che da insiemi predefiniti di regole e passaggi logici si trasformano in sistemi di intelligenza artificiale capaci di modificare autonomamente le proprie modalità di funzionamento. *Big data* e *machine learning* producono un salto quantico nell'universo della valutazione automatica, che passa da una valutazione di tipo additivo, esemplificata dai sistemi di *rating* che consentono agli utenti di valutare e recensire un servizio o un bene – si pensi a piattaforme come Tripadvisor, Yelp e Google Score – a valutazioni di tipo cibernetico, che si basano su processi inferenziali alimentati da un numero crescente di variabili e da articolati meccanismi di retroazione. Questo secondo tipo di sistemi è ciò che qui intendiamo per valutazione algoritmica, ossia un processo che non si limita ad assegnare punteggi sulla base di una sommatoria di valori predefiniti pur ponderati, ma che produce previsioni e decisioni sulla base di un sistema di indicatori doppiamente dinamico perché, da un lato, si nutre costantemente di nuovi dati raccolti dalle fonti più disparate d'informazione ed elaborati in un processo iterativo virtualmente senza fine, e dall'altro si modifica autonomamente grazie alle proprie capacità autoriflessive e di apprendimento.

Una delle prime e più note applicazioni di massa della valutazione algoritmica è quella sviluppata dal sistema finanziario per la gestione dei rischi legati all'erogazione dei prestiti ai privati. Complessi assemblaggi di software e banche dati valutano i profili dei clienti per determinarne il livello di affidabilità economica e, di conseguenza, stabilire i tassi d'interesse in maniera personalizzata. I cosiddetti *credit scoring systems*, adottati da banche e istituti finanziari a partire dal secondo dopoguerra negli Stati Uniti d'America (Abdou e Pointon 2011), si sono gradualmente sviluppati in articolati meccanismi di valutazione basati su algoritmi predittivi che elaborano grandi quantità d'informazioni personali per stimare le probabilità degli individui di restituire crediti, finanziamenti e mutui (Baesens *et al*. 2003, Citron e Pasquale 2014). Più di recente, anche le compagnie assicurative hanno iniziato a impiegare sistematicamente tecniche di *machine learning* per definire i premi da applicare ai clienti che sottoscrivono polizze auto, professionali o sulla vita, e per individuare automaticamente i tentativi di frode (Boodhun e Jayabalan 2018). Un altro settore in cui la valutazione algoritmica trova crescente applicazione è quello della selezione delle risorse umane. Ad oggi, più della metà delle agenzie di *human resource management* e la quasi totalità delle grandi *corporation* transnazionali utilizza software predittivi per identificare i soggetti a cui indirizzare gli annunci di lavoro, per prevedere la performance dei candidati, stimarne lo stipendio desiderato e decidere chi assumere e quali domande rigettare (Bogen e Rieke 2018). La valutazione algoritmica è prassi cruciale anche dei grandi siti del cosiddetto *Web 2.0*: motori di ricerca come Google e Yahoo!, social network come Facebook, Twitter e Instagram, *online marketplac*e come Amazon e Alibaba, siti di *user generated content* come YouTube e Vimeo, aggregatori di notizie come Google News, Feedly e Panda. Queste piattaforme, pur presentandosi come intermediari neutrali, in realtà decidono, attraverso un sistema sofisticato di regole algoritmiche dinamiche, cosa mostrare ai propri utenti, come e quando, con significativi effetti sul discorso pubblico, sulla produzione culturale e sulle relazioni sociali (Gillespie 2010, 2018).

Fin qui abbiamo citato casi di valutazione algoritmica che, pur avendo rilevanti conseguenze sociali (cfr. van Dijck, Poell, de Waal 2018), sono adottati e implementati da soggetti economici privati. Ma sempre più spesso gli algoritmi predittivi vengono impiegati anche da organizzazioni pubbliche e istituzioni in importanti processi di *decision-making*, come quelli relativi ai servizi sanitari, ai sussidi, all'assistenza sociale, alla protezione dei minori (Oswald 2018). Un chiaro esempio di questa tendenza è fornito dalla *Government Transformation Strategy* del governo britannico che pre-

vede l'adozione sistemica di modelli predittivi per «anticipare la domanda di servizi, o i cambiamenti di politiche, e prepararsi a venire incontro ai bisogni mutevoli dei cittadini e del business, informando le decisioni del governo su quali servizi offrire e su come farli funzionare» (UK Government 2017)[1]. I sistemi di valutazione algoritmica sono inoltre diventati elementi fondamentali delle politiche di controllo dell'immigrazione. Ad esempio, l'Unione Europea ha sviluppato numerosi strumenti di valutazione algoritmica per la gestione dei flussi migratori e dei controlli di frontiera, che consentono alle autorità preposte d'individuare i soggetti a più alto rischio durante le procedure di sbarco dei passeggeri di treni e aerei, di controllo doganale, di emissione dei divieti di ingresso, di presentazione delle domande di visto, residenza e asilo (FRA 2018, pp. 112 e segg.). Negli Stati Uniti, il programma *Secure Communities*, sperimentato nel 2008 dalla presidenza di George W. Bush, implementato su larga scala dall'amministrazione Obama nel 2011 e rilanciato nel 2017 dal *Department of Homeland Security* su ordine del presidente Trump, prevede l'integrazione dei database della polizia federale (*Federal Bureau of Investigation*, FBI), dell'agenzia di controllo delle frontiere e dell'immigrazione (*Immigration and Customs Enforcement*, ICE) e delle polizie statali per lo scambio d'informazioni e dati biometrici al fine di individuare gli immigrati irregolari più pericolosi, e di concentrare su di essi le attività di cattura e deportazione. Un altro ambito pubblico in cui la valutazione algoritmica si sta rapidamente istituzionalizzando è quello relativo all'amministrazione della giustizia penale. Molte corti statunitensi, ad esempio, utilizzano software che consentono di predire il rischio di recidiva di ciascun detenuto, e di decidere consequenzialmente in merito alla quantificazione della pena da comminare ai condannati o alle istanze di libertà condizionale (Christin, Rosenblat e Boyd 2015). Un altro caso di valutazione algoritmica applicato nell'ambito di servizi pubblici con un alto impatto sulla vita di comunità e individui è quello relativo all'esercizio delle funzioni di polizia, il cosiddetto *predictive policing,* che verrà analizzato e discusso in dettaglio nel prossimo paragrafo. Qui è utile sottolineare che l'adozione di sistemi di valutazione algoritmica da parte di autorità pubbliche non è un fenomeno esclusivo dell'occidente capitalista, ossia del luogo natio della governance neoliberale, ma va diffondendosi ovunque nel mondo, persino nella patria del comunismo sovranista, la Cina. Il famigerato *Social Credit System* è un apparato di valutazione della reputazione di individui, imprese e organizza-

1 Tutti i passaggi citati testualmente in questo saggio sono stati liberamente tradotti in italiano dall'autore.

zioni pubbliche attualmente sperimentato dal governo di Pechino in alcune aree del paese, che si basa sull'integrazione di database, *blacklist* e sistemi di monitoraggio e sorveglianza già esistenti, e che s'intende estendere a tutta la popolazione cinese entro il 2020 (Mac Síthigh e Siems 2019). L'obiettivo è quello di consolidare «la cultura della sincerità», «le virtù tradizionali», «una mentalità onesta», e «costruire un'armoniosa società socialista» (Consiglio di Stato Repubblica Popolare Cinese, 2014).

La restante parte dell'articolo analizzerà un tipo particolare di valutazione algoritmica, ossia quella utilizzata per la previsione dei fenomeni criminali. Quello del *predictive policing* è un caso cruciale che esemplifica, in un ambito gravido di conseguenze politiche e sociali, l'impatto e i limiti dei sistemi autonomi di valutazione e *decision-making*. In particolare, nel prossimo paragrafo verranno discussi definizioni, contesti, finalità, strumenti e approcci alle pratiche di polizia predittiva. Nel paragrafo successivo, sulla base di un recente filone di letteratura sia teorica che empirica, gli aspetti critici di tali pratiche verranno analizzati e sistematizzati, e infine generalizzati all'intero universo della valutazione algoritmica. Il paragrafo conclusivo riassume le sfide poste dai sistemi autonomi di valutazione alle società contemporanee, evidenziando lo scarto tra la velocità di sviluppo e adozione di queste nuove tecnologie e i tempi necessari a valutarne funzionamento ed effetti da una prospettiva politica di tipo democratico.

2. *La valutazione di luoghi e individui: la polizia predittiva*

Secondo una definizione ampiamente adottata in letteratura, per "polizia predittiva" s'intende «l'applicazione di tecniche d'analisi – in particolare tecniche quantitative – per identificare probabili obiettivi per gli interventi di polizia e prevenire il crimine o risolvere crimini passati attraverso predizioni statistiche» (Perry *et al*. 2013, pp.1-2). Una definizione più articolata, che coglie anche il background teorico e gli effetti pratici dei sistemi di valutazione algoritmica applicati alle funzioni di polizia, è quella proposta da Craig Uchida: «il *predictive policing* è una strategia multidisciplinare basata sull'applicazione della legge, che mette assieme tecnologie avanzate, teoria criminologica, analisi predittiva e operazioni tattiche che in definitiva conducono a risultati ed esiti come la riduzione del crimine, l'efficienza della gestione [delle forze di polizia], e comunità più sicure» (Uchida 2014, p. 3871). Un'altra definizione, che si basa su un'estesa revisione della letteratura e che sottolinea, a differenza delle altre, l'importanza della fase di raccolta delle informazioni che an-

dranno poi a confluire nel modello predittivo, è quella proposta da Meijer e Wessels, secondo i quali «il *predictive policing* è la raccolta e l'analisi di dati sui crimini passati per l'identificazione e la previsione statistica di individui o aree geospaziali con maggiore probabilità di attività criminale, al fine di aiutare a sviluppare interventi di polizia e strategie e tattiche di prevenzione» (Meijer e Wessels 2019, p. 3).

Al di là della singola definizione che s'intenda adottare, quello della previsione algoritmica del crimine è «un campo vasto e dai confini nebulosi» (Gerstner 2018, p. 116), i modelli statistici e le teorie criminologiche sottostanti i diversi approcci sono numerosi e spesso usati in combinazione tra loro, gli strumenti in uso variano in quanto a funzionalità, modalità di utilizzo e costi di sviluppo, e differenti sono anche le finalità della loro applicazione (Tab.1): predire luoghi e tempi dei reati, predire gli individui che commetteranno un reato in date condizioni, individuare i profili degli autori di crimini passati per confrontarli con quelli dei sospettati di un nuovo reato, predire le identità di individui e gruppi che hanno un'alta probabilità di essere vittime di azioni criminali (Perry *et al*. 2013). In generale, i software di *predicting policing* che aspirano a individuare le aree cittadine più a rischio utilizzano metodi come il *near-repeat*, che si basa sull'assunto che particolari tipi di reati tendano a ripetersi in una medesima zona, e come la *risk terrain analysis*, che invece considera gli attributi di un'area che favoriscono l'azione criminale come la presenza di locali notturni, di cantieri, banche, aree poco illuminate, ecc. Entrambi i metodi sono derivati da una teoria razionalista del soggetto criminale e dall'assunto che questi calcoli di volta in volta i rischi e gli incentivi connessi a ogni sua eventuale azione. I software finalizzati a predire i soggetti che hanno più alta probabilità di compiere un reato o quelli più a rischio di restarne vittime fanno invece sovente uso di *social network analysis*, sia sulla base di attività di intelligence, come spesso avviene per la prevenzione dei reati delle bande giovanili, sia sulla base di analisi condotte sui social media. In questo caso, la teoria di fondo dei modelli predittivi è la teoria delle reti sociali, che si basa sull'assunto che il comportamento individuale sia influenzato dalle relazioni sociali che veicolano valori, credenze, visioni del mondo e atteggiamenti, e che le azioni delle persone siano significativamente condizionate dal contesto interpersonale della propria vita quotidiana.

Tab. 1. Tipologia funzionale del predictive policing

Obiettivi	Teoria criminologica	Metodi d'analisi	Input	Sistemi (casi)
Previsioni spazio-temporali	Rational choice	Near-repeat	Storico dei reati, frequenza reati	Predpol
		Risk terrain	Storico dei reati, attributi geospaziali	Hunchlab
Profilazioni criminali e vittime	Social network	Social network analysis	Storico dei reati, social media, influencer, informazioni da data broker	Beware, Strategic Subjects List (SSL)

Al primo tipo di software di polizia predittiva, quello cioè orientato alle previsioni spazio-temporali del crimine, appartengono strumenti come PredPol e Hunchlab. PredPol è un software utilizzato in più di sessanta dipartimenti di polizia statunitensi che basa le sue previsioni sui dati storici delle attività criminali (tipo di crimine, luogo, data e ora) adoperando il metodo *near-repeat*. Hunchlab invece è un software che si basa sulla *risk terrain analysis* e che prende in esame un numero molto elevato di variabili, inclusi orari di apertura delle scuole, eventi sportivi, condizioni meteo, ecc. Il prodotto è sviluppato dalla società Azavea nota anche per un altro prodotto molto diffuso presso le centrali delle forze dell'ordine statunitensi, ShotSpotter, un sistema di sensoristica sonora in grado di rilevare e segnalare in tempo reale l'esplosione di colpi da arma da fuoco. Alla seconda categoria di sistemi di *predictive policing*, ossia quella che valuta i profili dei soggetti criminali, appartengono sistemi come Beware e la Strategic Subjects List (SSL). Beware è un algoritmo predittivo sviluppato dalla Intrado, oggi acquisita dalla West Corporation, che viene integrato nel sistema delle chiamate di emergenza del 911. Quando la centrale di polizia riceve una chiamata, il software elabora l'indirizzo presso cui viene richiesto l'intervento, recupera i nomi dei residenti, e per ciascuno di essi fornisce agli agenti una valutazione del livello di pericolosità su una scala cromatica: verde, giallo e rosso. Il sistema si basa su dati acquisiti da diversi *data broker*, da fonti aperte e dai social network. La Strategic Subjects

List del Dipartimento di polizia di Chicago, nota anche come Chicago Heat List, utilizza dati relativi ai precedenti penali dei cittadini e informazioni estratte dai social network per identificare le persone con elevata probabilità di commettere un crimine o di restarne vittime. Il sistema consente anche di individuare *influencer* del crimine, ossia membri delle gang giovanili che hanno un forte ascendente su altri giovani e che possono per questo indurli a compiere reati. Le persone così identificate vengono visitate frequentemente dalla polizia o raggiunte da una *Custom Notification Letter* che informa sulle pene connesse ai reati. I primi tre sistemi di *predictive policing* qui discussi – Predpol, Hunchlab e Beware – sono di proprietà delle aziende private che li hanno sviluppati, e funzionano in modalità *software as a service*: vengono installati sui server delle compagnie che detengono tutti i dati utilizzati dagli algoritmi di *machine learning*, mentre i dipartimenti di polizia fruiscono delle previsioni attraverso interfacce web. SSL è invece uno dei rari casi di *predictive policing* sviluppati all'interno del corpo di polizia che lo utilizza.

Attualmente, i sistemi di polizia predittiva sono impiegati in diverse parti del mondo, Europa compresa (in particolare in Germania e Svizzera), ma è negli Stati Uniti d'America che il loro dispiegamento presso i dipartimenti di polizia ha assunto dimensioni sistemiche. Grandi città come Chicago, Memphis, Los Angeles, Santa Cruz, Minneapolis, Palm Beach, Dallas, Baltimora, New York City, Philadelphia e Miami hanno sviluppato in proprio o, più frequentemente, acquistato da privati soluzioni informatiche per la previsione dei reati (Brayne, Rosenblat e Boyd 2015). Ratcliffe e Kikuchi (2019) rilevano che una simile tendenza affonda le sue radici non tanto nell'aumento, reale o percepito, del numero e dell'efferatezza dei crimini, quanto nelle politiche di austerità fiscale avviate dai governi USA a partire dagli anni '80, che hanno ridotto notevolmente i budget dei dipartimenti di polizia spingendo questi ultimi verso una ricerca frenetica di soluzioni in grado di incrementarne efficacia, efficienza ed economicità (cfr. anche Beck e McCue 2009). Egbert, analizzando il caso tedesco, nota come, accanto alla disponibilità tecnica di nuovi strumenti e alle già menzionate motivazioni di tipo economico, l'adozione di strumenti di *predictive policing* sia soprattutto il portato di ragioni politiche, e più nello specifico dell'opportunità offerta ai politici di mostrarsi all'elettorato come attenti alla sicurezza e capaci di proporre soluzioni innovative: «il *predictive policing* può dimostrarsi politicamente un successo senza praticamente funzionare, in quanto il messaggio simbolico di essere duri con il crimine può essere fatto circolare efficacemente anche se la stessa tecnologia non funziona (ancora) bene» (Egbert 2018, p. 108).

In generale, per quanto riguarda le tattiche implementate dalla polizia a seguito delle previsioni algoritmiche, gli approcci esistenti si possono distinguere in due macro-categorie: gli approcci preventivi, che mirano a far desistere gli autori del crimine, ad esempio dispiegando nelle aree cittadine più a rischio personale in divisa, o contattando di persona i soggetti con più alta probabilità di commettere reati per fargli sentire la pressione delle forze dell'ordine; e gli approcci repressivi, che invece intensificano un controllo di tipo discreto, o mimetico, sulle aree o sui soggetti segnalati dall'intelligenza artificiale. Dal punto vista tecnico, l'effettiva capacità dei programmi e dei modelli di *predictive policing* di individuare situazioni di rischio e di ridurre i livelli criminalità è stata testata sia in laboratorio che sul campo, conducendo a risultati contrastanti (cfr. Saunders, Hunt e Hollywood 2016; Meijer e Wessels 2019). Al di là degli effetti concreti sulla frequenza dei fenomeni criminali, si vuole qui sistematizzare e discutere le conseguenze sociali del *predictive policing* come caso specifico della valutazione algoritmica. In particolare, vedremo in seguito gli aspetti più critici della polizia predittiva evidenziati dalla letteratura e dalla ricerca empirica, e come questi aspetti siano generalizzabili a tutti i sistemi di valutazione algoritmica che si basano su assemblaggi tra *big data* e intelligenza artificiale.

3. *I rischi della valutazione algoritmica del rischio*

La letteratura accademica, le inchieste giornalistiche e gli esperimenti condotti sul *predictive policing* hanno evidenziato una lunga serie di problemi ed effetti collaterali connessi a questa nuova pratica di controllo e prevenzione del crimine. Un primo cluster di osservazioni critiche è stato sviluppato attorno al concetto di *bias*, ossia all'insieme di pregiudizi, distorsioni ed errori insiti nel modello predittivo, nelle raccolte di dati o ancora nelle modalità di funzionamento dell'algoritmo. Lum e Isaac (2016), analizzando l'algoritmo di Predpol e le banche dati della polizia di Oakland, hanno dimostrato che il *predictive policing* dei reati di droga tende a sottoporre a un controllo sproporzionato le comunità non bianche e a più basso reddito. Gli autori concludono che l'utilizzo di Predpol produca un circolo vizioso in cui i quartieri più poveri della città ricevono pattugliamenti più capillari da parte della polizia (*over-policing*), e ciò, a sua volta, rafforza il modello predittivo e la sua tendenza a sovra-rappresentare le probabilità che i crimini avvengano presso le comunità più marginali (*feedback loop*). Problemi simili sono stati riscontrati anche in altri sistemi di valutazione

algoritmica, come quelli utilizzati dalle corti statunitensi per predire le probabilità di recidiva dei detenuti. Un'inchiesta della *newsroom* ProPublica sul sistema *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS) ha dimostrato come, a parità di altre condizioni, le persone di colore vengano sistematicamente ritenute più pericolose dei bianchi (Angwin, Larson, Mattu e Kirchner 2016). Più in generale, Harini Suresh e John Guttag (2019) del Massachusetts Institute of Technology hanno individuato cinque fonti di *bias* nei sistemi di *machine learning*:

1) Bias storici, ossia pregiudizi che non sono attribuibili ad errori nella raccolta dei dati, ma alla realtà sociale e politica che i dati rappresentano, con un effetto discriminatorio ai danni di minoranze etniche e religiose, di donne, disabili, omosessuali e soggetti marginali;

2) Bias rappresentativi, che invece occorrono quando i *dataset* su cui l'algoritmo viene addestrato sono poco rappresentativi dell'effettiva popolazione su cui il sistema di *machine learning* dovrà operare;

3) Bias di misurazione, che si verificano quando una variabile è erroneamente utilizzata come proxy per misurare un altro fenomeno, come avviene, ad esempio, quando si usa il numero degli arresti effettuati in un'area come indicatore del numero di reati, o quando il numero di arrestati tra parenti e amici di un detenuto viene usato per predire il rischio di recidiva di quest'ultimo, così come avviene nel già citato sistema COMPAS;

4) Bias di aggregazione, che si hanno quando un modello predittivo sviluppato in un particolare contesto viene adottato in un contesto del tutto differente;

5) Bias di valutazione, che possono prodursi quando diversi sistemi predittivi vengono valutati rispetto a *benchmarks* e *best practices* sviluppati in contesti diversi secondo un modello *one-size-fits-all*.

Un altro problema connesso all'utilizzo dei sistemi di polizia predittiva riguarda l'opacità del loro funzionamento. Gran parte dei sistemi in uso, infatti, sono prodotti da compagnie private, che custodiscono gelosamente i propri codici sorgente per evitare che questi vengano duplicati o parzialmente copiati dai propri concorrenti. In molti casi, inoltre, come abbiamo visto in precedenza, persino i dati di cui si nutre il sistema di *machine learning* vengono archiviati ed elaborati sui sistemi proprietari delle aziende fornitrici, estromettendo di fatto l'autorità pubblica dalla gestione delle informazioni. Infine, è utile sottolineare come, pur disponendo dei codici sorgente e dei dati su cui i software operano, l'output di un processo di *machine learning* è per definizione difficile da ricondurre in maniera puntuale a una sequenza di decisioni, e il sistema predittivo si presenta come una scatola nera agli stessi soggetti che lo hanno costruito (House of Lords

Select Committee on Artificial Intelligence 2018; Burrell 2016). Come evidenziato da alcuni studiosi «[l]a mancanza di trasparenza e supervisione sulle pratiche e sulle politiche di polizia e sui dati creati per il loro tramite solleva serie preoccupazioni sulla possibilità che qualsiasi sistema predittivo che si basi sulle informazioni della polizia possa operare in maniera equa e giusta» (Richardson *et al.* 2019, p. 25). Il problema della trasparenza dei sistemi di valutazione algoritmica non riguarda soltanto il *predictive policing*, ma ha una portata molto più ampia:

> Questa opacità è diventata la norma per le istituzioni private. Non sorprendentemente, queste considerano i loro algoritmi una proprietà intellettuale, che è necessario tenere lontano dagli occhi dei loro concorrenti. Più sorprendentemente, le istituzioni pubbliche fanno lo stesso, proteggendo i propri algoritmi dalla ribalta. Unendosi a banche e compagnie assicurative, i dipartimenti delle entrate, della polizia, della sicurezza degli aeroporti mantengono nascosti i modelli che utilizzano (de Laat 2017, p. 526).

L'opacità degli algoritmi che misurano, valutano e decidono le sorti di prodotti, servizi, individui e istituzioni non è la conseguenza inevitabile di una traiettoria tecnologica o di uno sviluppo senza alternativa. Essa è piuttosto il portato delle strategie di segretezza implementate dalle grandi organizzazioni economiche, mediatiche e finanziarie dei nostri tempi, che hanno trasformato – e sempre più trasformano – le società contemporanee in «black box society» (Pasquale 2015).

Un importante corollario del problema dell'opacità dei sistemi di valutazione algoritmica è la loro inappellabilità, l'impossibilità di contestarne gli output laddove sia gli input sia il processo di elaborazione risultino inaccessibili. Come hanno argomentato Oswald, Grace, Urwin e Barnes:

> Se un algoritmo usato da agenti di polizia per plasmare i loro processi decisionali diventa nella pratica il produttore di una decisione indiscutibile da un utente umano […] un ricorrente in revisione giudiziaria può argomentare di essere stato soggetto a una decisione illegittima, resa illegale da un inappropriato 'condizionamento di discrezionalità'. Questo potrebbe anche essere il caso di un ricorrente che fronteggi l'esito di un processo decisionale fondato su algoritmi, con nessuna possibilità di contestare quella decisione (Oswald *et al*. 2018, p. 240).

Anche il problema della inappellabilità delle decisioni assunte da sistemi di intelligenza artificiale va ben oltre i confini incerti della polizia predittiva. Nella sua analisi dei modelli decisionali basati su *machine learning*, definiti «armi di distruzione matematica», Cathy O'Neil scrive: «Come

divinità, questi modelli matematici sono opachi, il loro funzionamento è invisibile a tutti fuorché ai più alti sacerdoti nel loro dominio: matematici e informatici. I loro verdetti, anche quando sbagliati o dannosi, sono al di là [di ogni possibile] contestazione o appello» (O'Neil 2016, p.3).

Un altro aspetto critico della polizia predittiva riguarda la sua stretta interconnessione con – o la sua dipendenza da – i sistemi di sorveglianza elettronica generalizzata. Abbiamo già osservato che alcuni sistemi di *predictive policing* attingono i dati su cui operano dai social media, da agenzie di *data brokering*, da fonti di intelligence e, come nel caso di ShootSpotter, da sistemi di sensoristica disseminati sul territorio urbano. A questi sistemi vanno ovviamente aggiunti i circuiti di videosorveglianza, le *fidelity card* che tracciano gli acquisti di beni e servizi, e le informazioni raccolte dalle compagnie telefoniche relative non solo al traffico dati o alle chiamate effettuate e ricevute, la cui conservazione – *data retention* – è divenuta obbligatoria per legge in moltissimi paesi, ma anche alla posizione e agli spostamenti degli individui, alla loro compresenza in specifici luoghi, agli orari di accesso ai servizi online, ai contenuti fruiti e pubblicati, ai siti web visitati, alle chiavi di ricerca utilizzate. Anche in questo caso, i sistemi di polizia predittiva rappresentano null'altro che un caso particolarmente emblematico di una tendenza più generale. Abbiamo già accennato al fatto che spesso la valutazione algoritmica si basa sulla raccolta e l'elaborazione di dati biometrici, come nel caso degli algoritmi utilizzati per il controllo dell'immigrazione illegale. Altri casi particolarmente emblematici riguardano i *credit score system* offerti da alcune *start-up* che controllano i *font* scaricati sui computer dei soggetti che richiedono prestiti o mutui per verificare la presenza dei caratteri tipicamente utilizzati dai siti web di scommesse e gioco d'azzardo (King 2014); oppure le conversioni forzate delle abitazioni in affitto in *smart home*, con l'installazione di serrature, termostati, allarmi e sensori per l'acqua interconnessi a banche dati centralizzate, che possono facilmente essere utilizzate dai proprietari degli immobili per la sorveglianza dei propri inquilini (Ng 2019). In termini più generali, la sorveglianza rappresenta il modello di business fondamentale della nuova economia digitale in quella che Shoshana Zuboff (2019) definisce «l'età del capitalismo della sorveglianza»:

> Il capitalismo della sorveglianza rivendica unilateralmente l'esperienza umana come materiale grezzo gratuito da traslare in dati comportamentali. Sebbene alcuni di questi dati siano impiegati per il miglioramento di prodotti o servizi, il resto è dichiarato surplus comportamentale proprietario, dato in pasto ad avanzati processi di costruzione noti come 'machine intelligence', e assemblati in prodotti-predizione che anticipano cosa farai ora, presto e dopo. Infine,

> queste previsioni sono scambiate in un nuovo tipo di mercato per previsioni comportamentali che definisco mercato dei futures comportamentali (Zuboff 2019, p. 6).

In modo simile, altri studiosi utilizzano il concetto di società della sorveglianza, concettualizzando quest'ultima come «il sistematico monitoraggio, ammassamento e studio dell'informazione per assumere decisioni, minimizzare il rischio, ordinare le popolazioni, ed esercitare il potere. Definiamo sorveglianza il monitoraggio delle persone per regolare o governare il loro comportamento» (Gilliom e Monahan 2013, p.2). Se la sorveglianza diffusa rappresenta un sistema invisibile di monitoraggio e controllo, la valutazione algoritmica che su di essa si fonda, al contrario, rende ovunque visibile lo status dell'individuo sottoposto a valutazione. Nel caso del *predictive policing*, le visite delle forze dell'ordine presso le abitazioni dei soggetti a rischio sono visibili al vicinato e ai passanti e, in un certo senso, annunciano al contesto di vita quotidiana della persona sottoposta a controllo la sua pericolosità, il suo status di rischio per la collettività (Degeling e Berendt 2018). Conseguenze simili si riscontrano anche nei sistemi di valutazione algoritmica adoperati per il controllo dell'immigrazione, che «rendono lo status di immigrato visibile, accessibile e rilevante in più domini sociali e legali che mai, e soggetto a monitoraggio e controllo da parte di un'ampia gamma di attori pubblici e privati» (Kalhan 2013, p. 1109).

Un ultimo aspetto critico della valutazione algoritmica è meritevole di attenzione: la «automazione dell'ineguaglianza», ossia la tendenza a utilizzare «l'alta tecnologia per profilare, sottoporre a controllo di polizia e punire i poveri» (Eubanks 2018). Anche in questo caso, non si tratta di una tendenza naturale, ma del portato di scelte politiche chiaramente discriminatorie. Alcuni *data scientists*, ad esempio, notando che «i sistemi di polizia predittiva si concentrano in maniera sproporzionata sui crimini di strada anziché sui reati da colletti bianchi» (Clifton *et al*. 2017) hanno sviluppato un'applicazione di polizia predittiva che segnala le aree metropolitane a più alto rischio di reati finanziari[2]. Ad oggi nessun dipartimento di polizia o agenzia federale sembra abbia adottato il sistema. Inoltre, va tenuto in considerazione che, per i motivi sopra esposti, contestare una decisione assunta da un sistema di valutazione algoritmica è difficile e costoso, e questo naturalmente crea una discriminazione tra chi ha le risorse economiche per intraprendere lunghe e dispendiose battaglie legali, e chi invece non possiede nemmeno gli strumenti culturali per riconoscere l'ingiustizia di

2 https://whitecollar.thenewinquiry.com/

cui è stato vittima. Infine, proprio in considerazione del fatto che i sistemi algoritmici di *decision-making* vengono spesso adottati come strumenti per ridurre i costi connessi alla valutazione umana, è molto più probabile che si venga sottoposti a valutazione algoritmica in contesti poveri di risorse che in ambienti elitari. Come scrive Kathy O'Neil in merito alle procedure di reclutamento: «Una prestigiosa agenzia di servizi professionali o un'esclusiva scuola privata propenderanno molto di più verso raccomandazioni e interviste faccia a faccia rispetto a una catena di fast-food o a un distretto scolastico urbano senza un quattrino. I privilegiati […] vengono trattati generalmente dalle persone, le masse dalle macchine» (O'Neil 2016, p. 6).

4. *Conclusioni*

La valutazione algoritmica sta rapidamente trasformando le modalità con cui le istituzioni pubbliche e private definiscono i problemi collettivi, valutano i possibili corsi d'azione, e infine assumono decisioni cruciali per il benessere di comunità, gruppi sociali e individui. Questa trasformazione ha ovunque caratteristiche ben precise: è generalmente condotta da soggetti economici privati che esercitano sempre più spesso funzioni pubbliche; è implementata a prescindere da valutazioni univoche sull'effettiva capacità degli strumenti adottati; è protetta da qualsivoglia forma di scrutinio pubblico; è legittimata da motivazioni economiche discendenti dal dogma monetarista dell'austerità e da motivazioni politiche di tipo securitario.

La delega dei processi decisionali all'automa valutante avviene inoltre in una cornice discorsiva che presenta la valutazione algoritmica come oggettiva, imparziale, frutto asettico di un calcolo che riduce, quando non annienta, la discrezionalità umana. Anzi, mentre l'errore e il pregiudizio umano diventano elementi intollerabili e inammissibili, e pertanto fungono da innesco delle istanze di automazione – il «soluzionismo» di cui parla Morozov (2013) – l'errore algoritmico è, nella migliore delle ipotesi, minimizzato come occasione di miglioramento del sistema e, nella peggiore, viene semplicemente occultato o negato. In realtà, come abbiamo osservato, gli errori e le conseguenze nefaste dei sistemi di valutazione algoritmica sono frequenti e di diversi tipi. In questo saggio abbiamo individuato cinque categorie di aspetti critici ed effetti perversi: la produzione e riproduzione di bias, l'opacità del funzionamento dei sistemi, l'incontestabilità delle valutazioni e delle decisioni, la dipendenza dagli apparati e dalle pratiche di sorveglianza, e la perpetuazione dell'ineguaglianza. Un sesto elemento che si è volutamente tralasciato in quanto esula dalle finalità del saggio, ma

che è utile qui brevemente richiamare, riguarda gli aspetti geopolitici della valutazione algoritmica. Gran parte degli analisti e osservatori, infatti, concorda sul fatto che la leadership mondiale nello sviluppo dell'intelligenza artificiale sia ormai in mano cinese (cfr. Duranton *et al*. 2018; Andriole 2018; Wu 2018; WIPO 2019). Questo trend lascia intravvedere, da un lato, una possibile riconfigurazione dei rapporti interstatali sulla base di una mutazione degli equilibri di potere e, dall'altro, un'evoluzione tutt'altro che democratica nelle modalità di produzione e negli ambiti di applicazione della valutazione algoritmica. Si consideri inoltre che, a seguito della combinazione tra robotica e intelligenza artificiale, gli algoritmi di valutazione vengono sempre più spesso integrati nei sistemi d'arma, e la realizzazione di *killer robot* in grado di valutare chi e quando rappresenti una minaccia, e di decidere autonomamente se aprire il fuoco e se uccidere o meno, è già una realtà rispetto alla quale la comunità internazionale stenta a trovare un accordo su un possibile framework normativo a protezione dei diritti umani (Scharre 2018).

In conclusione, la valutazione algoritmica rappresenta uno dei più importanti vettori trasformativi dei sistemi di governance contemporanei. Trainata dai nuovi *hype* tecnologici dell'intelligenza artificiale, del *machine learning*, del *deep learning* e degli algoritmi predittivi, l'adozione di apparati autonomi di valutazione procede a una velocità di gran lunga superiore a quella necessaria per indagarne gli effetti sociali e per sviluppare un dibattito pubblico adeguato alla formazione di una volontà politica consapevole e condivisa. Il caso del *predictive policing*, se da un lato è particolarmente emblematico per i suoi effetti sociali, è dall'altro solo uno dei tanti campi di applicazione della valutazione algoritmica. La trasformazione in atto è di amplissima portata, sfugge sistematicamente al controllo dei soggetti che ne subiscono gli effetti, e mal si presta ad essere governata attraverso processi politici fondati su principi democratici, sui diritti fondamentali e sulla *rule of law*. Le sfide che essa pone si ergono da territori inesplorati, all'incrocio tra governamentalità neoliberale ed esercizio della più brutale forma di sovranità.

Mauro Santaniello (msantaniello@unisa.it)
Internet & Communication Policy Centre
Dipartimento di Studi Politici e Sociali
Università degli Studi di Salerno

Riferimenti bibliografici

Abdou H., Pointon J., 2011, *Credit Scoring, Statistical Techniques and Evaluation Criteria: A Review of the Literature*, in «Intelligent Systems in Accounting, Finance & Management», n. 18 (2-3), pp. 59-88.

Andriole A., 2018, *Artificial Intelligence, China and the U.S. - How the U.S. Is Losing the Technology War*, in «Forbes», November 9, https://bit.ly/2FeUaGY, (consultato il 15 marzo 2019).

Angwin J., Larson J., Mattu S., Kirchner L., 2016, *Machine Bias: There's Software Used Across the Country to Predict Future Criminals and It's Biased Against Blacks*, in «ProPublica», May 23, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, (consultato il 15 marzo 2019).

Baesens B., VanGestel T., Viaene S., Stepanova M., Suykens J., Vanthienen J., 2003, *Benchmarking State-of-the-Art Classification Algorithms for Credit Scoring*, in «Journal of the Operational Research Society», n. 54, pp. 627–635.

Beck C., McCue C., 2009, *Predictive Policing: What Can We Learn from Wal-Mart and Amazon About Fighting Crime in a Recession?*, in «Police Chief», LXXVI, 11, pp. 1-7.

Bogen M., Rieke A., 2018, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, in «Upturn», https://www.upturn.org/reports/2018/hiring-algorithms (consultato il 15 marzo 2019).

Boodhun N., Jayabalan M., 2018, *Risk Prediction in Life Insurance Industry Using Supervised Learning Algorithms*, in «Complex & Intelligent Systems», n. 4, pp. 145-154.

Brayne S., Rosenblat A., boyd D., 2015, *Predictive Policing*, in «Primer for the Data & Civil Rights Conference: A New Era of Policing and Justice, Washington, D.C., October 27, 2015», http://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf , (consultato il 15 marzo 2019).

Burrell J., 2016, *How The Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, in «Big Data & Society», January – June, 10, pp. 1-12.

Christin A., Rosenblat A., boyd D., 2015, *Courts and Predictive Algorithms*, in «Primer for the Data & Civil Rights Conference: A New Era of Policing and Justice, Washington, D.C., October 27, 2015», http://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf , (consultato il 15 marzo 2019).

Citron K.C., Pasquale F.A., 2014, *The Scored Society: Due Process for Automated Predictions*, in «Washington Law Review», n. 89 (1), pp. 1-33.

Clifton B., Lavigne S., Tseng F., 2017, *Predicting Financial Crime: Augmenting the Predictive Policing Arsenal*, in «The New Inquiry», https://whitecollar.thenewinquiry.com/static/whitepaper.pdf , (consultato il 15 marzo 2019).

Consiglio di Stato Repubblica Popolare Cinese, 2014, *Planning Outline for the Construction of a Social Credit System (2014-2020)*, versione inglese https://bit.ly/1zO58fV, (consultato il 15 marzo 2019).

de Laat P.B., 2018, *Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?*, in «Philosophy & Technology», n. 4(31), pp. 525-541.

Degeling M., Berendt B., 2018, *What Is Wrong about Robocops as Consultants? A Technology-Centric Critique of Predictive Policing*, in «AI & Society», n.3(33), pp. 347–356.

Duranton S., Erlebach J., Pauly M., 2018, *Mind the (AI) Gap Leadership Makes the Difference*, Boston, Boston Consulting Group.

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

Eubanks V. 2018, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, New York, St. Martin's Press.

FRA - European Union Agency for Fundamental Rights, 2018, *Preventing Unlawful Profiling Today and in The Future: A Guide*, Luxembourg, Publications Office of the European Union.

Gerstner D., 2018, *Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany*, in «European Journal for Security Research», n. 3, pp. 115–138.

Gillespie T., 2010, *The Politics of 'Platforms'*, in «New Media & Society», n. 12(3), pp. 347–364.

Id., 2018, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, New Haven, Yale University Press.

Gilliom J., Monahan T., 2013, *SuperVision. An Introduction to the Surveillance Society*, Chicago, The University of Chicago Press.

House of Lords Select Committee on Artificial Intelligence, 2018, *AI in the UK: Ready, Willing and Able?*, Report of Session 2017–19, https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf, (consultato il 15 marzo 2019).

Kalhan A., 2013, *Immigration Policing and Federalism Through the Lens of Technology, Surveillance, and Privacy*, in «Drexel University School of Law Legal Studies Research Paper Series».

King J., 2014, *Credit Scoring for the Social Media Generation*, in «The Banker», https://bit.ly/2XYSk4h, (consultato il 15 marzo 2019).

Lum K., Isaac W., 2016, *To Predict and Serve?*, in «Significance», n.5(13), pp. 14-19.

Mac Síthigh D., Siems M., 2019, *The Chinese Social Credit System: A Model for Other Countries?*, European University Institute, Department of Law, Working Paper LAW 2019/01.

Meijer A., Wessels M., 2019, *Predictive Policing: Review of Benefits and Drawbacks*, in «International Journal of Public Administration», DOI: 10.1080/01900692.2019.1575664

Morozov E., 2013, *To Save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems That Don't Exist*, London, Allen Lane.

Ng A., 2019, *Your Landlord Turns Your Apartment into a Smart Home. Now What?*, in «CNet», March 7, https://www.cnet.com/news/your-landlord-

turns-your-apartment-into-a-smart-home-now-what/ (consultato il 15 marzo 2019).

O'Neil C., 2016, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, NY: Broadway Books.

Oswald M., 2018, *Algorithm-Assisted Decision-Making in the Public Sector: Framing the Issues Using Administrative Law Rules Governing Discretionary Power*, in «Philosophical Transactions of the Royal Society», n. 2128(376), pp. 1-20.

Oswald M., Grace J., Urwin S., Barnes G.C., 2018, *Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality*, in «Information & Communications Technology Law», n. 27(2), pp. 223-250.

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

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

Ratcliffe J.H., Kikuchi G., 2019, *Harm-Focused Offender Triage and Prioritization: A Philadelphia Case Study,* in «Policing: An International Journal», https://doi.org/10.1108/PIJPSM-08-2018-0118.

Richardson R., Schultz J., Crawford K., 2019, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, in «New York University Law Review Online», Forthcoming, https://ssrn.com/abstract=3333423 (consultato il 15 marzo 2019).

Saunders J., Hunt P., Hollywood J.S., 2016, *Predictions Put into Practice: A Quasi-Experimental Evaluation of Chicago's Predictive Policing Pilot*, in «Journal of Experimental Criminology», n. 3(12), pp. 347-371.

Scharre P., 2018, *Army of None: Autonomous Weapons and the Future of War*, New York, W. W. Norton & Company.

Suresh H., Guttag J.V., 2019, *A Framework for Understanding Unintended Consequences of Machine Learning*, in «arXiv.org», https://arxiv.org/abs/1901.10002, (consultato il 15 marzo 2019).

Uchida C., 2014, *Predictive Policing*, in Bruinsma G., Weisburd D. (a cura di) *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, pp. 3871-3880.

UK Government, 2017, *Government Transformation Strategy: Better Use of Data*, https://bit.ly/2LiU0il (consultato il 15 marzo 2019).

van Dijck J., Poell T., de Waal M., 2018, *The Platform Society: Public Values in a Connective World*, Oxford, Oxford University Press.

WIPO – World Intellectual Property Organization, 2019, *Artificial Intelligence*, https://www.wipo.int/publications/en/details.jsp?id=4386, (consultato il 15 marzo 2019).

Wu H., 2018, *China Is Achieving AI Dominance by Relying on Young Blue-Collar Workers*, in «Motherboard», December 21, https://bit.ly/2FgLgZv, (consultato il 15 marzo 2019).

Zuboff S., 2019, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, New York, Public Affairs.

Finito di stampare
nel mese di novembre 2019
da Geca Industrie Grafiche – San Giuliano Milanese (MI))