Predictive policing: trasparenza degli algoritmi, impatto sulla privacy e risvolti discriminatori

Beatrice Perego*

PREDICTIVE POLICING: ALGORITHM TRANSPARENCY, PRIVACY IMPACT AND DISCRIMINATORY IMPLICATIONS

ABSTRACT: Police departments around the world are embracing new predictive policing technology that will help them spot criminals before the crime takes place. Predictive analysis provides tools that have the potential to improve the efficiency of law enforcement, however, this outcome ultimately depends on the human beings' understanding of the inherent limitations of such tools in order to avoid ineffective and unfair results. This brief analysis seeks to highlight the potential risks arising from the use of predictive policing, with specific reference to the processing of personal data, the lack of algorithm transparency and the discriminatory consequences.

KEYWORDS: Predictive policing; machine learning; privacy; bias; algorithm transparency

1. Introduzione

Quadrati rossi sparsi su *Google maps* e la polizia si precipita nell'area indicata per fermare i criminali prima che il reato abbia luogo. Sembra che la finzione di Minority Report[1] sia diventata realtà. Le previsioni sono elaborate da algoritmi inseriti in software utilizzati in tutto il mondo e che sono alla base della *predictive policing*, termine che descrive un sistema di analisi dei dati volto alla creazione di modelli predittivi che indicano dove può verificarsi un crimine o chi potrebbe esserne coinvolto[2]. Così, l'assunto tradizionale dell'impossibilità di prevedere il

**Dottoressa in Giurisprudenza, Università degli studi di Trento. Mail: beatrice.perego@alumni.unitn.it .*

[1] Minority Report è un film di fantascienza americano del 2002 diretto da Steven Spielberg e basato sul racconto "The Minority Report" di Philip K. Dick: nel 2054, un dipartimento di polizia specializzato (PreCrime), grazie alle conoscenze fornite dai cosiddetti "precogs", arresta i criminali prima ancora che i crimini vengano commessi. Uno dei temi principali affrontati dal film è il ruolo dell'attività di governo preventivo nella protezione dei cittadini, in uno stato futuro basato sulla tecnologia. In particolare, il film evidenzia come tali sviluppi tecnologici rendano la presenza del governo quasi illimitata e si interroga sul'eventuale legalità di un "procuratore infallibile".

[2] Perry et al. descrivono il controllo predittivo come «the application of analytical techniques — particularly quantitative techniques — to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions». W.L. PERRY, B. MCINNIS, C.C. PRICE, S. SMITH, J.S. HOLLYWOOD, *Predictive Policing:*

comportamento umano – da sempre tenuto separato dai fenomeni chimici o fisici sulla base della capacità di autodeterminazione dell'uomo – con la stessa accuratezza delle leggi della natura, sembra crollare di fronte all'avvento delle nuove tecnologie[3] e l'ormai diffuso impiego dell'analisi predittiva[4]. Molto spesso i crimini non sono casuali ma seguono dei modelli e, di fatto, esiste un forte *corpus* di prove a sostegno della teoria secondo cui la criminalità è prevedibile (in senso statistico), e ciò in quanto i criminali tendono a porre in atto il tipo di crimini che hanno commesso con successo in passato, generalmente vicino allo stesso luogo e nello stesso periodo temporale[5]. Così, Jeff Brantingham, antropologo che ha aiutato a supervisionare il progetto di polizia predittiva per il Los Angeles Police Department, sostiene che «humans are not nearly as random as we think. In a sense, crime is just a physical process, and if you can explain how offenders move and how they mix with their victims, you can understand an incredible amount[6]». Anche se questo non è universalmente vero, si verifica con una frequenza sufficiente a far funzionare ragionevolmente le tecniche di apprendimento automatico utilizzate nei sistemi di polizia predittiva. L'obiettivo è quello di identificare le aree in cui alcuni tipi di reati sono frequenti e prevenirne il ripetersi. Ciò può servire come preziosa fonte di conoscenza per le forze dell'ordine a livello strategico: analizzando tale tecnologia dalla prospettiva della polizia tradizionale, la mappatura predittiva può aiutare un dipartimento ad assegnare le pattuglie in modo più

The Role of Crime Forecasting in Law Enforcement Operations, Santa Monica, CA: *RAND Corporation*, 2013, cit. 1 ss., www.rand.org (10/05/2020). Ancora, il vicedirettore di NIJ, John Morgan, lo definisce come «any policing strategy or tactic that develops and uses information and advanced analysis to inform forward-thinking crime prevention». C.D. UCHIDA, *A National Discussion of Predictive Policing: Defining Our Terms and Mapping Successful Implementation Strategies,* in *Justice & Security Strategies*, 2009, cit. 1. L'autrice Beth Pearsall definisce il controllo predittivo come «taking data from disparate sources, analyzing them and then using results to anticipate, prevent and respond more effectively to future crime». B. PEARSALL, *Predictive Policing: The Future of Law Enforcement?*, in *National Institute of Justice Journal*, 2010.

[3] Cfr. A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà,* in *BioLaw Journal,* 2019; Vedi anche S. CASSESE, *Il diritto nello specchio di Sofocle*, in *Il Corriere della Sera*, 2018.

[4] Con il termine predictive analytics si indicano diverse tecniche di *Machine Learning*, tra cui il *Data Mining*, le quali includono tipicamente algoritmi di apprendimento automatico che eseguono l'estrazione dei dati e l'analisi statistica, determinando collegamenti e tendenze nei dati, per creare modelli predittivi. Cfr. M. KANTARDZIC, *Data Mining: Concepts, Models, Methods, and Algorithms*, *Hoboken*, 2011, 6; C. MCCUE, *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis, Burlinghton*, 2006.

[5] Le tecniche di polizia predittiva sono, infatti, radicate in una serie di teorie criminologiche -teoria della vittimizzazione ripetuta, della disorganizzazione sociale ed efficacia collettiva, della scelta razionale e dell'attività di routine- che i ricercatori della RAND corporation hanno consolidato in quella che chiamano teoria mista in base alla quale criminali e vittime seguono modelli di vita comuni, i quali, se analizzati congiuntamente indicano un aumento delle probabilità di reato. Inoltre le caratteristiche geografiche e temporali influenzano il dove e quando di tali modelli. Infine viene sottolineato come i criminali, mentre si muovono all'interno di questi modelli, prendano decisioni "razionali" riguardo a se commettere reati, tenendo conto di fattori quali l'area, l'idoneità dell'obiettivo e il rischio di essere scoperti. W.L. PERRY et al. *op. cit,* 2-3. Per un riassunto delle teorie del comportamento criminale vedi R.V. CLARKE, M. FELSON, *Routine Activity and Rational Choic*e, New Brunswick, 2003; C.D. UCHIDA, *Encyclopedia of Criminology and Criminal Justice*, Thousand Oaks, 2014.

[6] V. J. RUBIN, *Stopping Crime Before It Starts*, *in Los Angeles Times*, 2010. www.latimes.com (15/03/2020); Così, ad esempio,«In 2009, the Chicago Police Department received a $2 million grant from the National Institute of Justice to develop a predictive program for crime. The theory behind Chicago's winning application was that with enough research and data they might be able to demonstrate that the spread of crime, like epidemics, follows certain patterns. It can be predicted and, hopefully, prevented». C. O'NEIL, *Weapons of math destruction. How Big data increases inequality and threatens democracy*, New York, 2016, 98 ss.

efficiente e a ridurre i tempi di risposta; da un punto di vista proattivo, le azioni di polizia possono essere potenziate da una scansione più accurata delle aree con problemi di criminalità dal momento che alcuni dei metodi predittivi impiegati forniscono anche informazioni sugli indicatori principali –o variabili esplicative – , offrendo la possibilità non solo di prevedere i crimini futuri, ma anche di identificare le cause sottostanti alla criminalità[7].

2. Gli attuali sistemi predittivi

Quello svolto dai software predittivi, a ben vedere, appare come una replica del lavoro precedentemente riservato ai soli operatori umani. Le previsioni circa i luoghi e le persone coinvolte in attività criminali sono sempre state parte dell'attività di polizia, la differenza risiede nel fatto che gli algoritmi di analisi lavorano con dati ad alta dimensione, il che comporta una logica decisionale qualitativamente diversa applicata a input maggiori. A oggi, inoltre, la qualità delle previsioni è notevolmente migliorata grazie alla combinazione di due fattori: il primo si riferisce alla disponibilità di strumenti (computer) sempre più potenti, veloci e con elevatissime capacità di memoria (e quindi anche di archiviazione); il secondo è rappresentato dall'enorme quantità di dati provenienti da fonti diverse[8]. La disponibilità dei c.d. Big Data[9] consente, infatti, di sviluppare profili individuali basati su attività criminali passate, associazioni attuali e altri fattori legati al pericolo sociale e all'inclinazione criminale. Questo è il motivo per cui le forze dell'ordine, come parte di una grande spinta verso una polizia proattiva, stanno cambiando la sorveglianza e le risorse investigative per concentrarsi sulla previsione. Resta da sottolineare come non sia disponibile un modello standardizzato di polizia predittiva ma, al contrario, l'attività svolta dipende sia dal metodo predittivo impiegato, sia dalle tipologie di dati utilizzati dal sistema[10].

---

[7] Sul tema si veda in generale J.M. CAPLAN, L.W. KENNEDY, J.D. BARNUM, E.L. PIZA, *Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis to Explore the Dynamics of Criminogenic Behavior Setting*, in *Journal of Contemporary Criminal Justice*, 2017, 133 ss.; J.M. CAPLAN, L.W. KENNEDY, *Risk Terrain Modeling: Crime Prediction and Risk Reduction*, in *University of California Press*, 2016; L.W. KENNEDY, J.M. CAPLAN, E.L. PIZA, *Risk Clusters, Hotspots and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies*, in *Journal of Quantitative Criminology*, 2010, 339 ss.

[8] F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto penale e Uomo*, 2019, 6, disponibile a questo indirizzo www.penalecontemporaneo.it: «dalla digitalizzazione di documenti o generati da ognuno di noi scattando foto, facendo video o inviando messaggi tramite le reti sociali o altri strumenti di messaggistica, come Whatsapp, Messenger, etc. (c.d. dati people-to-people); oppure dati raccolti da istituzioni pubbliche o soggetti privati, inerenti i cittadini o gli utenti, come dati fiscali, sanitari, ricerche sul web, transazioni commerciali, bancarie (c.d. dati people-to-machine); infine, dati di tipo machine-tomachine, generati, automaticamente e indipendentemente dall'intervento di esseri umani, da dispositivi fisici, come ad esempio vari tipi di sensori, dispositivi di geo-localizzazione, werables, smart devices, tra di loro connessi nell'Internet delle Cose»; Circa l'internet delle cose v. N. CLIMER, *Il cloud e l'Internet delle cose*, in J. AL-KHALILI (a cura di), *Il futuro che verrà*, Torino, 2017, 133 ss.

[9] «Big Data represents the Information assets characterized by such a High Volume, Velocity and Variety to require specific Technology and Analytical Methods for its transformation into Value». A. DE MAURO, M. GRECO, M. GRIMALDI, *What is Big Data? A Consensual Definition and a Review of Key Research Topics*, *in ResearchGate*, 2014, 8

[10] I ricercatori della RAND Corporation hanno identificato «four broad categories: 1. Methods for predicting crimes: These are approaches used to forecast places and times with an increased risk of crime. 2. Methods for predicting offenders: These approaches identify individuals at risk of offending in the future. 3. Methods for

Le forme più comuni di *predictive policing* in uso sono quelle note come metodi "*place based*". Il fulcro dell'attività di polizia *place-based* è l'attenzione a determinati luoghi nei quali convergono una serie di fattori che rendono l'area ad alto rischio o tasso di criminalità[11]. Le tecniche impiegate possono essere semplici come il pattugliamento dei punti caldi (c.d. *hot spot*)[12], ma la polizia locale può anche adottare un approccio più complesso, orientato alla valorizzazione di una strategia specifica per ciascuna delle piccole aree ad alto rischio[13]. Le tattiche esatte adottate possono quindi variare, così come possono variare gli indici principali e i dati inseriti nei software predittivi usati dalle forze dell'ordine: ad esempio, i software di hot spot come PredPol[14] elaborano le previsioni sulla base di dati storici della criminalità; altri software utilizzano dati più esoterici – come le condizioni meteorologiche, l'illuminazione stradale, la vicinanza a negozi di liquori, ecc. – per arrivare alle loro previsioni del crimine e un esempio in questo senso è rappresentato dal software Risk Terrain Modeling Diagnostics (RTMDx) Utility[15]. Dal punto di vista di un agente di polizia, l'*output* del modello di *risk terrain* sarà qualitativamente uguale a quello di un metodo *hot spot*: entrambi evidenziano aree che sono probabilmente soggette a un alto tasso di criminalità nel prossimo futuro. Tuttavia, dal punto di vista dell'analista, si tratta di metodi

predicting perpetrators' identities: These techniques are used to create profiles that accurately match likely offenders with specific past crimes. 4. Methods for predicting victims of crimes: Similar to those methods that focus on offenders, crime locations, and times of heightened risk, these approaches are used to identify groups or, in some cases, individuals who are likely to become victims of crime». W.L. PERRY, B. MCINNIS, C.C. PRICE, S.C. SMITH, J.S. HOLLYWOOD, *op. cit*., xiv-xv. Cfr. anche C. O'NEIL, *op. cit.*, 87 ss.

[11] J. BACHNER, *Predictive Policing: Preventing Crime with Data and Analytics*, Washington, 2013.

[12] Un esempio è il caso dell'Hot Spots Policing Experiment di Minneapolis. Si veda L.W. SHERMAN, D. WEISBURD, *General deterrent effects of police patrol in crime hot spots: A randomized controlled trial*, in *Justice Quarterly*, Vol. 12, 1995. Lo studio conclude che un aumento sostanziale della presenza di pattuglie di polizia può effettivamente causare modeste riduzioni della criminalità e riduzioni più consistenti del disordine all'interno di luoghi ad alta criminalità.

[13] Un esempio è il Jersey City Problem-Oriented Policing Project. Cfr. A.A. BRAGA, D.L. WEISBURD, E.J. WARING, L.G. MAZEROLLE, W. SPELMAN, F. GAJEWSKI, *Problem-oriented policing in violent crime places: A randomized controlled experiment*, in *Criminology*, 37, 1999. Questo esperimento randomizzato si premurava di generare maggiori conoscenze sull'utilità di interventi problem-oriented per controllare i luoghi con un alto tasso di attività criminale violenta. Lo studio ha concluso che il programma pilota di polizia "orientato ai problemi" del Jersey City Police Department è riuscito a ridurre il numero totale di incidenti criminali e il numero totale di chiamate di servizio.

[14] www.predpol.com (23/03/2020): «utilizzando solo tre tipologie di dati – tipo di reato, data/ora del reato e luogo del reato – per fare previsioni, la tecnologia *PredPol* ha aiutato le forze dell'ordine a ridurre drasticamente il tasso di criminalità in giurisdizioni di tutti i tipi e di tutte le dimensioni, negli Stati Uniti e all'estero. *PredPol* può vantare una comprovata sperimentazione: il Dipartimento della polizia di Los Angeles ha registrato un calo del 20% dei reati previsti di anno in anno […] Il Dipartimento dello Sceriffo della contea di Jefferson ha registrato una riduzione del 24% nelle rapine e una riduzione del 13% nei furti con scasso. A Plainfield, New Jersey, da quando si usa *PredPol* si è avuta una riduzione del 54% delle rapine e una riduzione del 69% dei furti di auto».

[15] Il sistema RTMDx, lanciato dai ricercatori di Rutger, utilizza un algoritmo per testare empiricamente una varietà di influenze spaziali ed incrementa l' analisi per ogni fattore di rischio, al fine di identificare dove emergeranno nuovi episodi criminali o dove questi si raggruppano. La tecnica di risk terrain modelling può essere applicata a qualsiasi estensione geografica (locale, regionale, globale, urbana, suburbana, rurale, terrestre, marittima). Può essere utilizzato per analizzare quasi tutti gli argomenti. I dati relativi all'argomento rappresentano il problema o la questione che si intende analizzare (ad esempio, luoghi di incidenti di rapine, incidenti stradali o overdose di droga). dati sull'uso che sono rappresentativi dell'intera area di studio (ad esempio, negozi, stazioni di servizio, bar, parcheggi, scuole, ecc...) www.riskterrainmodeling.com (27/03/2020).

molto diversi. I metodi *hot spot* sono fondamentalmente tecniche di *clustering*[16] che segnalano le aree in cui si sono verificati gruppi di reati, mentre quello della la c.d *risk terrain analysis* è un approccio di classificazione che caratterizza il rischio di reato di un'area sulla base delle sue caratteristiche ed aiuta a identificare e comunicare i fattori ambientali associati ad eventi specifici[17].

La seconda macro-categoria di software predittivi si rifà all'idea del *crime linking*, ovvero all'idea che alcune fattispecie criminose si manifestino in un'area geografica e in un arco temporale circoscritti[18], il che rende possibile identificare le serie criminali, profilarne l'autore e prevedere le mosse future di quel soggetto specifico. Riconducibile a questa categoria è Keycrime[19], software in dotazione esclusiva della questura di Milano, il quale ha portato a risultati particolarmente significativi[20]. L'efficacia di Keycrime è stata vagliata da una ricerca condotta dalla Essex University e lo studio ha evidenziato come, mentre gli altri software di polizia predittiva lavorano su base puramente statistica al fine di individuare dove, quando e che tipo di crimine è probabile venga commesso, Keycrime definisce anche come una determinata fattispecie criminosa viene realizzata [21]. L'obiettivo del software è di prevedere dove colpirà l'individuo che si sta cercando, essendo in grado di attribuire alla persona fermata la responsabilità penale anche di altri crimini compiuti in precedenza, portando a giudizio un soggetto non per un solo evento, ma per una serie di eventi. Quello di Keycrime si mostra come un modello innovativo, che presenta un notevole interesse in quanto strutturato per una duplice finalità: sia di polizia di prevenzione[22] che polizia giudiziaria[23].

---

[16] I metodi di clustering suddividono i dati in gruppi in cui le informazioni sono "simili" matematicamente. Questi modelli fanno previsioni affermando che una situazione futura sarà probabilmente simile ad un gruppo di situazioni precedenti. W.L. PERRY et al. *op. cit*, 35.

[17] Cfr. J. SZKOLA, E.L. PIZA, G. DRAWVE, *Risk Terrain Modeling: Seasonality and Predictive Validity*, in *Taylor & Francis Online*, 2019; G. DRAWVE, S.C. MOAK, E.R. BERTHELOT, *Predictability of gun crimes: a comparison of hot spot and risk terrain modelling techniques*, in *Taylor & Francis Online*, 2014, 312 ss.; L.W. KENNEDY, J.M. CAPLAN, E.L. PIZA, *Risk Clusters, Hotspots and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies*, in *Journal of Quantitative Criminology*, 2010, 339 ss; V. più in generale *sub*. 8.

[18] Sulla teoria della "repeat victimization" vedi D.L. WEISEL*, Analyzing repeat victimization*, COPS U.S. Deparment of Justice, 2005, 4 ss; K.J. BOWERS, S.D. JOHNSON, Who *commits near repeats? A test of the boost explanation*, in *Western Criminology Review*, 2004.

[19] M. VENTURI, *KeyCrime La chiave del crimine*, introduzione di M. BENEDETTI, in *Profiling I Profili dell'abuso*, 2014.

[20] G. SANTUCCI, *Milano. Il programma anti rapine diventa una startup della sicurezza,* in *Corriere della Sera*, 2019; C. MORABITO, *La chiave del crimine*, in *Polizia moderna*, 2015. www.poliziadistato.it (27/03/2020); M. SERRA, *Rapinatore seriale catturato grazie al software "Key crime*", in *La Stampa*, 2018.

[21] Il punto di forza di questo software, rispetto ai competitor, sta nell'analisi dei tratti psicologici e delle modalità comportamentali dell'autore: il nucleo centrale delle informazioni raccolte è rappresentato dalle interviste delle vittime -svolte una volta trascorse almeno 24 ore dal fatto, così che non siano inficiate dallo stress post-traumatico- per cogliere eventuali sfumature del comportamento dell'autore così da individuare lo schema d'azione e prevedere dove e quando quel soggetto colpirà nuovamente. G. MASTROBUONI, *Crime is terribly revealing: Information technology and Police productivity*, 2017, 9 ss, disponibile pdf pdfs.semanticscholar.org (27/03/2020). Contiene ed espone i risultati della ricerca condotta per conto della Essex University.

[22] Nel caso in esame, inoltre, a differenza che per i sistemi di *hot spot*, l'analisi non si basa solo sulla probabilità statistica data dal numero di episodi commessi da un soggetto o da persone che vivono in un determinato quartiere e non è previsto un sistema di autoalimentazione delle percentuali dei crimini commessi. In questo modo si evita il fenomeno della c.d. "*self fulfilling prophecy*". V. più approfonditamente par. 3.3.

[23] Ora, se il modello descritto non pone particolari problemi dal punto di vista della polizia di prevenzione, lo stesso non si può dire con riguardo alla seconda finalità, ovvero quella di ricostruzione di una serie criminale

In ogni caso, sebbene l'uso di software predittivi sia in parte motivato dal desiderio di correggere l'azione umana, di per sé fallibile, resta da considerare che, lungi dall'essere strumenti oggettivi o neutrali, quelli in esame condividono o, addirittura, amplificano molte delle debolezze del processo decisionale umano[24], sollevando diverse perplessità avendo riguardo al diritto alla privacy, alla trasparenza, e al principio di non-discriminazione.

3. L'impatto dei sistemi di *predictive policy* sull'individuo: privacy, trasparenza dell'algoritmo e discriminazione

Il controllo predittivo fornisce strumenti che hanno il potenziale per influenzare gli sviluppi della scienza dei dati al fine di migliorare l'efficacia e l'efficienza delle forze dell'ordine. Tuttavia, ciò dipende, in ultima analisi, dalla comprensione da parte degli esseri umani dei limiti intrinseci degli strumenti predittivi e delle conseguenze generate dal loro utilizzo: le prime preoccupazioni sono legate al modo in cui vengono raccolti i dati, con specifico riferimento al diritto di ogni individuo alla privacy nonché alla difficoltà di ottenere dati accurati e "puliti" da integrare in un sistema predittivo; in secondo luogo, non è chiaro come funzioni l'algoritmo in quanto non fornisce una spiegazione trasparente dei risultati che elabora, circostanza che compromette la capacità delle forze dell'ordine di rendere conto delle loro decisioni e dei destinatari di contestarle; infine, dal tipo di dati inseriti nel software e dal loro trattamento derivano quali sono le effettive operazioni di polizia, le quali possono rivelarsi discriminatorie[25].

3.1. Raccolta dei dati e diritto alla privacy

L'uso di tecniche che comportano la raccolta di un elevato volume di dati, la loro conservazione, il controllo incrociato delle banche dati e, più specificamente, la profilazione sistematica ai fini di un

riconducendo ad un soggetto una serie di eventi del passato immagazzinati nella banca dati. Occorre quindi chiedersi se, e in che termini, le informazioni contenute nel database possono entrare in un'annotazione della p.g. quale elemento di prova al fine dell'esercizio penale, per una richiesta di misura cautelare o ancora per un'intercettazione. Se nella prospettiva della polizia di prevenzione tutto il materiale acquisito e analizzato può essere utilizzato per le finalità perseguite, per la polizia giudiziaria solo le informazioni acquisite secondo quanto stabilito dalla disciplina codicistica potranno essere usate correttamente, senza incorrere in un formale divieto di utilizzabilità(ex art. 191 c.p.p.). Inoltre gli elementi che sono posti alla base della ricerca di pattern e correlazioni devono poter essere, in astratto, portati all'attenzione del giudice, il quale deve poter valutare: 1) in base a quali criteri è stata eseguita l'analisi comparativa che ha portato a mettere in evidenza determinate relazioni che si assumono rilevanti sul piano dalla ricostruzione della responsabilità; 2) in base a quali criteri tali relazioni possono costituire il fondamento della responsabilità penale in termini di certezza o elevata probabilità.

[24] In questo senso si veda E. STRADELLA, *Stereotipi e discriminazioni: dall'intelligenza umana all'intelligenza artificiale*, in *Consulta online (liber amico rum per Pasquale Costanzo)*, 2020, 3; G. NOTO LA DIEGA, *Against Algorithmic Decision-making, in Northcolumbia Legal Studies Working Paper Series, 2018, 3 ss.; G. NOTO LA DIEGA, Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information, in Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2018, 7 ss, disponibile al seguente indirizzo papers.ssrn.com (03/06/2020).

[25] H.V. JAGADISH, *The Promise and Perils of Predictive Policing Based on Big Data*, in *The Conversation*, 2015. gizmodo.com (30/03/2020); R. VAN BRAKEL, P. DE HERT, *Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies*, in *ResearchGate*, 2011, 163-192.

controllo predittivo, produce potenziali interferenze nel diritto alla privacy e nel trattamento dei dati personali[26]. In particolare, il termine profilazione si riferisce al *cross-check*, attraverso algoritmi, dei dati raccolti da varie fonti, al fine di prevedere il verificarsi di reati e la loro localizzazione (crime hot spot), ovvero la stesura del profilo penale individuale[27]. Quando si combinano e creano previsioni composite di una persona, tali analisi hanno conseguenze molto gravi per i destinatari e questo in particolare quando l'utilizzo delle informazioni raccolte non è sostenuto da una normativa in grado di garantire una tutela piena ed efficace della privacy. Da qui la scelta europea di adottare un approccio c.d. "espansionistico" di protezione dei dati personali, contrapposto al "riduzionismo" statunitense[28]. Ad esempio, nel 2012, nella sentenza della Corte Suprema degli Stati Uniti nella causa United States v. Jones, il parere concorde della giudice Sonia Sotomayor ha espresso serie preoccupazioni circa le invasioni della privacy che potrebbero derivare dalla raccolta diretta di enormi quantità di dati personali, in particolare, avendo riguardo alla capacità del governo di «raccogliere dati che rivelano aspetti privati dell'identità», attraverso mezzi come il monitoraggio del Global Position System (GPS)[29]. Attraverso i tools di polizia predittiva, il governo non solo sta guardando e raccogliendo enormi quantità

[26] Y. MONTJOYE, C.A. HIDALGO, M. VERLEYSEN, V.D. BLONDEL, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, in *Nature*, 2013. (spiega come l'uso dei Big Data può re-identificare i dati del telefono cellulare per tracciare gli individui); I database esistenti, come i dati sui crimini storici, migliorano la capacità di Big Data di collegare gli individui con le informazioni disponibili. Si veda anche A.G. FERGUSON., *Predictive Policing and Reasonable Suspicion*, in *Emory Law Journal*, 2012. Disponibile pdf in SSNR: papers.ssrn.com (01/04/2020).

[27] A. BABUTA, *Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities*, in *Royal United Services Institute for Defence and Security Studies*, 2017; M. MENDOLA, *One Step Further in the 'Surveillance Society': The Case of Predictive Policing*, in *Tech and Law Center*, 2016; P. DE HERT, H. LAMMERANT, *Predictive Policing and it's legal limits: effectiveness gone forever?,* in B. VAN DER SLOOT, D. BROEDERS, E. SCHRIJVERS (a cura di), *Exploring the boundaries of Big Data*, Amsterdam, 2016; K.C. BAUMGARTNER, S. FERRARI, G. PALERMO, *Constructing Bayesias Networks for criminal profiling from limited data*, in *Knowledge-Based System (Science Direct*), 2008; B.E. HARCOURT, *Against prediction. Profiling, policing and punishing in an actuarial age*, Chicago, 2007; K.C. BAUMGARTNER, S. FERRARI, C.G. SALFATI, *Bayesian Network Modeling of offender behaviour for Criminal profiling*, Siviglia, 2005.

[28] P.M. SCHWARTZ, D.J. SOLOVE, T*he PII Problem: Privacy and a new concept of personally identifiable information*, in *New York University Law Qaterly Review*, 2011.

[29] U.S . Supreme Court, United States v. Jones, N. 10-1259, 23- 01- 2012. Antoine Jones possedeva un nightclub nel Distretto di Columbia e nel 2004, una task force congiunta del Federal Bureau of Investigation (FBI) e del Metropolitan Police Department ha iniziato a indagare su lui per traffico di stupefacenti. Nel corso dell'indagine, un dispositivo GPS (Global Positioning System) è stato installato sull'auto di Jones, senza un mandato valido,. che ha monitorato i movimenti del veicolo 24 ore al giorno per quattro settimane. Il 23 gennaio 2012, la Corte Suprema ha ritenuto che «l'installazione da parte del Governo di un dispositivo GPS sul veicolo di destinazione, e il suo utilizzo per monitorare i movimenti del veicolo, costituisce una "ricerca" ai sensi del quarto emendamento». Tutti e nove i giudici hanno unanimemente considerato incostituzionale l'azione della polizia nei confronti di Jones, benché si trovassero in disaccordo sulle ragioni fondamentali della loro conclusione. Rimaneva, tuttavia, senza risposta -nonostante le preoccupazioni sollevate dalla giudice Sonia Sotomayor- la questione più ampia relativa alle implicazioni sulla privacy di un uso ingiustificato dei dati GPS in assenza di intrusione fisica - come potrebbe verificarsi, ad esempio, con la raccolta elettronica dei dati GPS dai fornitori di servizi senza fili o dai servizi di localizzazione e navigazione dei veicoli installati in fabbrica: la Corte ha infatti affermato che «It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question».

d'informazioni sugli individui, ma sta anche usando l'analisi predittiva per generare «dati che rivelano aspetti privati dell'identità[30]».

Analisi di questo tipo, negli Stati Uniti, sono utilizzate nei "centri di fusione", e cioè nei centri di informazione creati dal Dipartimento della Sicurezza Nazionale degli Stati Uniti e dal Dipartimento di giustizia per condividere i dati personali in possesso di agenzie come la CIA (Central Intelligence Agency), l'FBI (Federal Bureau of Investigation) e l'esercito[31]. L'aggregazione di dati di varie agenzie permette alle forze dell'ordine di prevedere o contrassegnare le persone come sospette, con la possibilità di sottoporle ad indagine, perquisizione, o detenzione in base ai criteri delineati dall'agenzia[32]. Tuttavia, a oggi non esistono norme o pratiche uniformi per guidare i servizi di polizia, pertanto la raccolta dei dati che saranno utilizzati come input per l'analisi statistica è rimessa, sostanzialmente, alla discrezionalità delle singole agenzie: di fatto, vi è l'idea errata che le forze dell'ordine locali siano tenute a conformarsi agli standard del programma Uniform Crime Reporting (UCR) del Federal Bureau of Investigation (FBI) per classificare i crimini[33]. Quando si esamina il Manuale UCR, infatti, diventa chiaro che questo programma è permissivo, e l'FBI, semplicemente, raccomanda che le agenzie si conformino al suo sistema di classificazione[34]. Quindi, le forze dell'ordine godono di discrezionalità nell'individuazione e dei dati del crimine da utilizzare, e ciò anche quando li segnalano all'FBI nell'ambito del programma UCR[35]. Inoltre, le questioni relative ai limiti costituzionali sulla sorveglianza dei dati pubblici, come il tracciamento GPS o le tecnologie di riconoscimento facciale[36] continuano a mettere alla prova l'interpretazione dei precedenti del quarto emendamento da parte dei tribunali[37], e ciò in quanto la mancanza di una legislazione completa sulla privacy[38], insieme al sistema di controllo giurisdizionale

[30] *Id*.

[31] D. GRAY, D. CITRON, *The Right to Quantitative Privacy*, in *Minnesota Law Review, Vol. 98,* Disponibile in SSRN papers.ssrn.com (01/04/2020).

[32] *Id.* Questo metodo può, tuttavia, portare a risultati errati: In un caso, la polizia di stato del Maryland ha sfruttato l'accesso ai centri di fusione per sorvegliare dei gruppi per i diritti umani, attivisti per la pace e oppositori della pena di morte per un periodo di diciannove mesi. Cinquantatre attivisti politici alla fine sono stati classificati come "terroristi", tra cui due suore cattoliche e una candidata democratica per una carica locale. Il centro di fusione ha condiviso queste erronee classificazioni terroristiche con le forze dell'ordine federali, i database delle forze dell'ordine e la National Security Administration, il tutto senza dare agli obiettivi innocenti alcuna opportunità di conoscere, e tanto meno correggere, il record. Vedi D.K. CITRON, F.A. PASQUALE, Network *Accountability for the Domestic Intelligence Apparatus* ,in *Hastings Law Journal*, Vol. 62, 2011, 1462. Disponibile in SSRN: papers.ssrn.com (01/04/2020).

[33] Uniform Crime Reports, Federal Bureu of investigation. www.fbi.gov (01/04/2020).

[34] A Word About UCR Data, Federal Bureau of investigation, www.fbi.gov (01/04/2020).

[35] *Id.*

[36] Cfr. paragrafo 3.3. del presente contributo.

[37] Supreme Court of. U.S., United States v. Jones, N. 10–1259, 23- 01- 2012; U.S Court of Appeals (3d. Circ.), United States v. Katzin, N. 12-2548, 19- 03- 2013 (controversia circa la possibilità che i dati GPS possano essere inclusi come prova se le autorità li hanno ottenuti senza un mandato).

[38] Nella seconda metà del XX secolo, grazie al suo vantaggio tecnologico sul resto del mondo, Washington ha assunto un ruolo guida nella protezione dei dati, per poi essere seguita (e forse sostituita) dalle istituzioni europee. Il quadro giuridico statunitense sulla privacy dei dati è costituito da un mosaico di tre tessere che comprende: strumenti legislativi, cause legali e, in misura minore, diritti costituzionali. V.E. ELMARADO, *Data Protection Law in the United States*, in *Academia*, www.academia.edu (03/04/2020); Tuttavia, ad oggi gli Stati Uniti sono ancora privi di una normativa generale sulla privacy, ma hanno adottato una discreta quantità di leggi che regolano specifici traffici di dati. Di conseguenza, la legislazione sulla privacy ha assunto la forma di una rete,

statunitense, ha fatto del quarto emendamento il fulcro della protezione dei dati personali[39]. La complessa ma incompleta, natura della legge statunitense sulla privacy dei dati è stata spesso criticata dai commentatori[40] per aver preferito gli interessi economici e di sicurezza alle libertà individuali[41]. È risaputo che gli uffici federali sono molto impegnati in attività di ricerca di dati, raccogliendo ogni tipo d'informazioni, indipendentemente dal loro rapporto con lo scopo della misura da adottare[42]. Tuttavia, oltre alle difficoltà strutturali, la sfida principale che gli Stati Uniti si trovano ora ad affrontare sono le loro misure di sicurezza. Nel 2013 la pubblicazione di alcuni documenti riservati da parte di Edward Snowden ha rivelato il sistema di sorveglianza da parte della National Security Agency (NSA) di cittadini americani e stranieri i cui dati sono stati raccolti su server americani. Lo scandalo internazionale (c.d. Datagate) ha messo in evidenza la scelta del governo statunitense di dare maggior peso agli interessi

riducendo gradualmente le dimensioni delle maglie ad ogni nuovo atto. Dopo l'FCRA (Fair Credit Reporting Act) del 1970 e Il PA (Privacy Act) del 1974, è stata la volta del Family Educational Rights and Privacy Protection Act (FERPPA) dello stesso anno. Il FERPA del 1974 si è occupato della privacy degli archivi scolastici degli studenti, assegnando la sua supervisione al Dipartimento dell'Educazione. Per accedere a tali dati era necessario un ordine giudiziario o una citazione legale. V. U.S. Code § 1232g , Family educational and privacy rights; Tuttavia, ad ogni nuovo atto legislativo si poneva un altro problema: l'assenza di un'Autorità di vigilanza comune. Infatti, a seconda del settore (economia, sanità, sanità, welfare, ecc.), ogni insieme di dati ha requisiti diversi per rivolgersi alla rispettiva Autorità, un disegno probabilmente efficace (l' Health Insurance Portability and Accountability Act (HIPAA) sotto la supervisione del Dipartimento della sorveglianza sanitaria, il FERPA al Dipartimento dell'educazione, il FCRA sotto Commissione federale del commercio, ecc.).

[39] R.J. PELTZ-STEELE, *The Pond Betwixt: Differences in the US-EU Data Protection/Safe Harbor Negotiation,* in *Journal of Internet Law*, 2015, 22 e ss. Il quarto emendamento della U.S. Constitution ha l'obiettivo finale di proteggere il diritto alla privacy e la libertà delle persone da intrusioni irragionevoli da parte del governo e recita «The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized». Nel testo, l'autore sottolinea come «Barring application of the odd sectoral statute, such as the Privacy Protection Act of 1980, which protects journalists, government intelligence gathering and criminal investigation are limited principally by the Fourth Amendment.», tuttavia, viene sottolineato come «the Fourth Amendment merely offers a constitutional floor to protect civil liberties, and the judicial process is far too slow to respond to new technological threats while people's liberty hangs in the balance. Americans should demand legislation to protect civil liberties above the floor, Crawford asserted. Beyond law enforcement, the Privacy Act of 1974 holds federal government agencies at least to standards that modestly resemble the contemporary fair information practices of Safe Harbor and the European Directive. [...] the United States should look hard at the Privacy Act. Its dated standards, only modestly amended since 1974, hardly suffice to protect personal privacy in the information age. In demonstrating respect for the dignity of the individual, government should set the example for private business, not trail behind. Even pending legislative action, the US executive has ample latitude in its oversight of federal record management to improve information practices with respect to personal privacy».

[40] *Id*; F. BIGNAMI, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, in *Boston College Law Review*, 2017.

[41] Tuttavia questo non ha impedito alla magistratura in United States v. Jones, di chiedere di ripensare l'applicazione del quarto emendamento alla luce dell'espansione delle nuove tecnologie.

[42] J. ROBINSON, *The Snowden Disconnect: When the Ends Justify the Means*, in *SSRN*, 2014. Tuttavia, questo non significa che non ci sia dibattito all'interno della comunità accademica degli Stati Uniti, né che la magistratura abbia abbracciato ciecamente la "causa della sicurezza". Vedi D.J. SOLOVE, *Nothing to Hide: The False Tradeoff Between Privacy and Security,* in *Yale University Press*, 2011. Disponibile su SSNR papers.ssrn.com (03/04/2020); L.P. VANONI, *Il Quarto emendamento della Costituzione americana tra terrorismo internazionale e datagate: Security v. Privacy*, in *Federalismi.it,* 2015.

di sicurezza nazionale rispetto che alla privacy[43], con la successiva abrogazione da parte della Corte di Giustizia della decisione 2000/520/CE della Commissione Europea sulla trasmissione dei dati dall'UE agli USA.

Così, non appena l'Unione ha riconosciuto che la rapidità della rivoluzione tecnologica stava modificando radicalmente i diritti dei cittadini europei, ha annunciato un progetto di legislazione sulle nuove forme di riservatezza dei dati. Anzitutto, dopo il trattato di Lisbona, la Carta dei diritti fondamentali dell'Unione europea (CFREU) è stata aggiunta alla legislazione primaria e la stessa Carta, all'art. 8[44], menziona esplicitamente la protezione dei dati come diritto fondamentale. In secondo luogo, a livello di diritto derivato, alcune garanzie circa l'utilizzo di *tools* predittivi si possono riscontrare nel "*data protection reform package*", rappresentato dal regolamento 2016/679/UE (GDPR) e dalla direttiva 2016/680/UE[45]. In particolare, il regolamento UE 2016/679, conosciuto come GDPR, stabilisce le norme generali per il trattamento, l'individuazione e l'aggiornamento dei dati personali. A oggi è

[43] D. OMBRES, *NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History,Constitutional Basis, and the Efforts at Reform*, in *Seton Hall Legis Journal*, 39, 2015, 27 ss.

[44] Art. 8 CFREU: «1. Everyone has the right to the protection of personal data concerning him or her; 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; 3. Compliance with these rules shall be subject to control by an independent authority».

[45] Quello della protezione dei dati personali è un tema verso il quale l'Unione presta particolare attenzione: si pensi al recepimento nel *Bill of Rights* dell'Unione europea di uno specifico diritto alla protezione dei dati (art. 8 C.d.f.u.e), nonché alla stessa giurisprudenza della Corte di Giustizia. Cft. G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, e O. POLLICINO, M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, entrambi in *G. RESTA, V. ZENO-ZENCOVICH (a cura di), La protezione transnazionale dei dati personali dai "safe Harbour principles" al "privacy shield", in Roma TR-Press, 2016.* A livello di diritto derivato, come accennato, alcune garanzie fondamentali si possono riscontrare nel regolamento 2016/679/UE (GDPR) e nella direttiva 2016/680/UE, i quali, rispettivamente agli artt. 22 e 11, sanciscono il divieto di decisioni basate unicamente su trattamenti automatizzati. Tale divieto risulta essenziale per scongiurare la c.d. *automation complacency* o *automation bias,* e cioè la tendenza dell'uomo ad accettare passivamente la decisione generata da una macchina senza cercare metterla in discussione ricercando elementi che possano contraddirla. Cfr. M.L. CUMMINGS, *Automation Bias in Intelligent Time Critical Decision Support Systems*, in *American Institute for Aeronautics and Astronautics*, 2004, disponibile a questo indirizzo citeseerx.ist.psu.edu (30/12/2019): «Automation bias occurs in decision-making because humans have a tendency to disregard or not search for contradictory information in light of a computer generated solution that is accepted as correct»; In secondo luogo, il divieto è motivato dalla necessità di decisioni ancorate al caso concreto, nonché dei requisiti richiesti per la motivazione -tra gli altri, il contatto diretto tra "giudice uomo" e l'individuo che egli andrà a giudicare, circostanza essenziale per la salvaguardia della dignità umana: solo se giudicato da un uomo, con una decisione suscettibile di critica, l'individuo non incorre in quel processo di «spersonalizzazione» nel quale «scompare la persona del decisore, sostituito appunto da procedure automatizzate; e scompare la persona in sé considerata, trasformata in oggetto di poteri incontrollabili» che contraddirebbe l'essenza stessa del giudizio. RODOTÀ, *Il diritto di avere diritti*, Bari, 2012, 401; Cfr anche E. NOVI, *Garapon: «la tecnologia non potrà mai sostituire giudice e avvocato»*, in *Il Dubbio*, 2018: «La tecnologia non potrà mai sostituirsi alla giustizia, perché carattere ontologico di quest'ultima è quello di dialogare con le passioni umane. Queste ultime prendono la forma, innanzitutto, di una aspettativa molto forte di giustizia, che poi altro non è che ciò gli americani chiamano *to have one's day in court,* ossia la possibilità di essere ascoltati, unita alla sensazione che "giustizia è stata fatta". Questo sentimento scaturisce da un evento sociale e la tecnologia digitale non può identificarsi in alcun modo con un fenomeno sociale: non vi è, al suo interno, uno spazio condiviso, non vi è alcun faccia a faccia, non c'è nessuna materialità».

possibile ottenere informazioni altamente riservate semplicemente attraverso un controllo incrociato di dati apparentemente innocui, non considerati sensibili, né personali dalla legislazione comunitaria o nazionale. Questo fenomeno è stato facilitato dai Big Data[46], che raccolgono e conservano continuamente informazioni per poi farle analizzare dai Data Brokers[47]. Pertanto, il regolamento ha ampliato la nozione di dati personali, comprese le informazioni relative a una persona fisica identificata o identificabile, tenendo conto di tutte le informazioni che possono portare all'identificazione di una persona mediante un controllo incrociato[48]. Inoltre, ciò che dovrebbe servire da garanzia per l'individuo è la cosiddetta pseudononimizzazione[49], la quale consiste nel «trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a una specifica persona senza l'uso di informazioni supplementari, a condizione che tali informazioni […] siano soggette a misure tecniche e organizzative per garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile[50]». Dunque, a livello europeo è stato adottato un modello di tutela dei dati personali, che si contrappone a quello statunitense, dove la tendenza è di considerare le PII solo come quei dati associati ad una persona specifica, lasciando così molte informazioni personali senza protezioni legali[51]: nell'approccio

[46] G. D'Acquisto, M. Naldi, *Big data e privacy by design*, Torino, 2017, 59 ss.

[47] S. Calzolaio, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *Federalismi.it,*, 2017; *Privacy by Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics*, in *European Union Agency for network and information security,* 2015.

[48] G. Giannone Codiglione, Risk-based approach *e trattamento dei dati personali*, in S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della* privacy, Padova, 2016.

[49] «Pseudonymization is a data management procedure by which personally identifiable information fields within a consumer data record are replaced by one or more artificial identifiers, or pseudonyms, which may be recalled at a later date to re-identify the record. Anonymization is the process of either encrypting or removing personally identifiable information from data sets so that the people whom the data describes remain permanently anonymous. […]Both methods involve masking personal data by removing or encrypting the data that makes it possible to link the information to an individual, such as name, address, or credit card number. However, the difference between the two is that pseudonymization can be reversed. Using separately held information, such as an encryption key, one can retrieve the identifiable information when needed to link the data back to an individual. Once data has been anonymized, however, it can never be linked back to an individual. Anonymization is permanent»: www.termsfeed.com (04/04/2020); V. anche https://gdpr.report/news/2017/11/07/data-masking-anonymisation-pseudonymisation/ (04/04/2020).

[50] Direttiva (EU) del Parlamento europeo e del Consiglio n. 680/2016, art. 3, par. 5. La direttiva ha ad oggetto la protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento di reati o dell'esecuzione di sanzioni penali, nonché la libera circolazione di tali dati, e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[51] Tuttavia si evidenziano le recenti iniziative legislative che riflettono una crescente e legittima volontà di implementare l'eticità e la legalità dell'IA. I senatori Cory Booker e Ron Wyden hanno proposto l'Algorithmic Accountability Act del 2019, primo sforzo legislativo federale per regolamentare i sistemi di IA Le entità che sviluppano, acquisiscono e/o utilizzano l'IA devono essere a conoscenza dei rischi derivanti dal suo utilizzo (e quindi di risultati e decisioni potenzialmente distorti) e impegnarsi per mitigare,nonché adottare azioni correttive, a fronte di eventuali pregiudizi. Così la legge autorizza e dirige la Federal Trade Commission ("FTC") a emettere e far rispettare i regolamenti che richiederanno a determinate persone, partnership e società di utilizzare, conservare o condividere le informazioni personali dei consumatori per condurre valutazioni d'impatto e "affrontare in modo ragionevole e tempestivo" eventuali pregiudizi o problemi di sicurezza identificati. V. Senate Bill 1108, 116th Congress, To direct the Federal Trade Commission to require entities that use, store, or share personal information to

comunitario è irrilevante se le informazioni siano già state collegate a un determinato soggetto, o potrebbero esserlo in futuro, i dati identificati e identificabili sono considerati come equivalenti[52]. Tuttavia, la pseudonimizzazione non garantisce l'anonimato assoluto e definitivo[53], in quanto, come già evidenziato, esiste la possibilità di una nuova identificazione delle persone attraverso il confronto incrociato di diverse tipologie di dati anonimi che possono far risalire le informazioni a un singolo individuo o a un profilo criminale[54]. Questo è il motivo per cui le tecniche di polizia predittiva dovrebbero essere condotte con «maggiore responsabilità algoritmica e trasparenza[55]».

3.2. Elaborazione dei dati e trasparenza dell'algoritmo

La scrutabilità dei risultati, valutata in termini di trasparenza od opacità degli algoritmi, si è rivelata una delle principali preoccupazioni legate all'utilizzo dei sistemi di polizia predittiva. Tale requisito si rivela di fondamentale importanza poiché gli algoritmi, poco prevedibili o spiegabili, sono difficili da controllare, monitorare e correggere. La trasparenza è generalmente definita rispetto a «la disponibilità di informazioni, le condizioni di accessibilità e come le informazioni [...] possono supportare in modo pragmatico o epistemico il processo decisionale dell'utente[56]». Il valore della trasparenza per il controllo predittivo si rivela, quindi, estremamente significativo, affinché questo sia utilizzato in modo efficace, legale ed etico[57]. Tuttavia, allo stato attuale delle tecnologie impiegate, esiste una mancanza di trasparenza a tutti i livelli di polizia predittiva. Anche qualcosa di semplice come le statistiche sulla criminalità, che in molti casi sono pubblicamente disponibili, continua a suscitare preoccupazioni circa

conduct automated decision system impact assessments and data protection impact assessments, 04/10/2019. www.wyden.senate.gov (12/05/2020).

[52] P.M. SCHWARTZ, D.J. SOLOVE, *op.cit.*, 1817; Cfr anche *R. DUCATO, La crisi della definizione di dato personale nell'era del web 3.0. Una lettura civilistica in chiave comparata*, in F. CORTESE, M. TOMASI (a cura di), *Le definizioni del diritto*, *Università degli Studi di Trento*, 2016, 160: «Molto articolata è la costruzione europea che mira ad inglobare quei dati e quelle informazioni che anche indirettamente possono essere ricollegati ad un determinato soggetto, così identificandolo. La nozione di PII, invece, è più ristretta perché prende in considerazione soltanto il dato riconducibile ad un soggetto identificato e non anche potenzialmente identificabile. Pertanto, mentre il sistema europeo mette al centro l'individuo, attraverso l'attrazione nell'ambito della normativa sulla protezione dei dati personali di tutta quell'informazione che possa riferirsi ad una persona identificata o identificabile (assicurando in quest'ultimo caso una copertura quasi totale contro le potenziali situazioni pregiudizievoli), il sistema statunitense mette in esponente la libertà di circolazione dell'informazione, dal momento che, adottando un approccio "riduzionista", la legislazione statale o federale risulta applicabile di fatto solo se i dati identificano un soggetto».

[53] G. DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018, 156 ss.

[54] A fronte dei nuovi sviluppi tecnologici «l'utilizzo e l'analisi di dati aggregati può comunque avere delle conseguenze lesive sulle persone cui quei dati si riferivano, potendo essere alla base di scelte inerenti un determinato gruppo etnico o linguistico o, ancora, potendo condizionare decisioni politiche ed economiche» e dunque si evidenzia la potenziale lesione degli interessi dei singoli quali membri di una comunità. Cft *R.* DUCATO*, op. cit.,* 153.

[55] European Parliament, *Report on fundamental rights implications of big data: privacy, data protection, nondiscrimination, security and law-enforcement*, cit., par. 8.

[56] Le componenti primarie della trasparenza sono, quindi, l'accessibilità e la comprensione delle informazioni. Vedi M. TURILLI, L. FLORIDI, *The ethics of informationtransparency*, in *Ethics and Information Technology*, 2009, 106.

[57] G. NOTO LA DIEGA, *Against Algorithmic Decision-making*, in *Northcolumbia Legal Studies Working Paper Series*, 2018, 4; V. in generale T. Z. ZARSKY, *Transparent Predictions, University of Illinois Law Review*, 2013.

l'accuratezza e la completezza[58]. L'aggiunta di dossier di dati personali crea nuovi problemi, in quanto il volume delle informazioni complica la valutazione trasparente delle fonti alla base delle previsioni[59]. Inoltre, pregiudizi personali o culturali non intenzionali possono "contaminare" i dati, i sistemi di *scoring*, i codici sorgente, e quindi i risultati predittivi che ne derivano[60]. In altre parole, senza investimenti significativi nell'esporre i metodi di raccolta dei dati, e senza un uguale investimento nella comprensione delle sfide associate all'inserimento e all'analisi dei dati, l'intero sistema corre il rischio di essere costruito su un database sconosciuto e non conoscibile[61]. Da un lato, alcune aziende rivendicano il diritto di mantenere il codice sorgente per sé stesse, trattando i loro algoritmi come segreti commerciali[62]. Dall'altro, la ragione tecnica di tale mancanza di trasparenza è legata al fenomeno della scatola nera (*black box*) e quindi, in molti casi in cui vengono impiegate tecnologie basate su algoritmi, gli agenti di polizia coinvolti nel funzionamento dei programmi non avranno alcuna comprensione di come lavora l'algoritmo[63]. Si tratta di un problema serio, dal momento che, quando lo Stato limita i diritti dell'individuo, deve esistere una base giuridica per tale restrizione al fine di proteggere le persone da un trattamento diverso in base a fattori arbitrari o illogici, come il luogo in cui vivono o la loro razza[64]. Questo è il motivo per cui gli investimenti nella polizia dovrebbero concentrarsi sullo sviluppo di programmi e algoritmi in grado di ridurre gli approcci parziali, lavorando per affrontare e limitare l'uso di informazioni viziate. In primo luogo, risulta fondamentale un sistema di audit indipendente che copra l'intero processo di raccolta, analisi e manutenzione dei dati, cioè si dovrebbero creare sistemi di

[58] J.F. GILSINAN, *The Numbers Dilemma: The Chimera of Modern Police Accountability Systems*, in St. *Louis University Public Law Review*, 2012. scholarship.law.slu.edu (07/04/2020).

[59] «The sheer volume of big data and the complexity of algorithms used to analyze it complicate transparency in data collection and use, and the rapidly increasing volume of aggregated personal data increases the risks of data security breaches for consumers.» A.M. SMITH, P. GILBERT, *Privacy and Fair Credit Reporting Act Update—2014*, in the *Business Lawyer, Vol. 70,* 2015, 585-86 www.cov.com (07/04/2020).

[60] Cfr. G. NOTO LA DIEGA, *Against the Dehumanisation of Decision-Making*, 33:«The trust in artificial intelligence and algorithms derives from the belief that non-human agents are unbiased, and their decisions are not affected by passions and ideologies. In fact, algorithms are as biased as the people who trained them, but in a less transparent and accountable way. The more important algorithms will become, the more we will want them to embed our values (and, therefore, our ideologies and biases). Further research should be carried out by diverse (also in terms of gender, ethnicity, etc.) multidisciplinary teams in order to find solutions to open the technical, organisation, and legal black boxes and to ensure fair algorithmic decision-making. Indeed, only a strong humanist stance will be able to reduce algorithmic bias».

[61] W.A. LOGAN, A.G. FERGUSON, *Policing Criminal Justice Data*, in *Minnesota Law Review*, 2016, 545-55; E. STRADELLA, *op. cit,* 5-7; B. FRIEDMAN, H. NISSENBAUM, *Bias in computer systems*, in *ACM Transactions on Information Systems (TOIS)*, 1996, 330 ss.

[62] E.E. JOH, The Undue Influence of Surveillance Technology Companies on Policing, in New York University Law Review Online, 2017, papers.ssrn.com: «police department may rely increasingly on big data tools, they do not create them. The police are costumers who contract with private vendors» which guard their algorithms as trade secret.

[63] Anche per i programmatori stessi, il processo decisionale algoritmico può essere difficile da decifrare: dunque avere accesso all'algoritmo utilizzato non significa che ci sarà un maggior grado di trasparenza perché spiegare come i dati vengono poi utilizzati e come funziona l'algoritmo rimane una questione incredibilmente difficile. Cfr. W.A. LOGAN, A.G. FERGUSON, op cit; G. NOTO LA DIEGA, *Against Algorithmic Decision-making*, in *Northcolumbia Legal Studies Working Paper Series*, 2018, 4 ss.

[64] *Sub*. 58.

conformità in grado di verificare se e come i dati vengano raccolti, registrati e inseriti nel sistema[65]. In secondo luogo, le metriche (ovvero i criteri sulla base dei quali lavora l'algoritmo) dovrebbero essere rese pubbliche[66]: un sistema può dirsi trasparente se fornisce un modo per dimostrare che la polizia predittiva funziona. Si rende, quindi, necessaria l'adozione di criteri misurabili e valutabili affinché si possa esprimere un giudizio di efficacia[67].

Ora, se da un lato la trasparenza può aiutare a prevenire la discriminazione e la stigmatizzazione – ad esempio attraverso la scelta delle variabili da parte del programmatore e i metodi di raccolta dei dati –, dall'altro, è anche improbabile che corregga il difetto di applicazione. Quindi, al fine di prevenire conseguenze dannose per i diritti individuali, è necessario che i programmi di polizia predittiva siano attuati in modo trasparente ma ciò non è sufficiente: se non porta alla correzione di distorsioni codificate nei dati o all'uso di informazioni "sporche", la trasparenza risulta piuttosto vuota come principio istituzionale.

3.3. *Dirty data* e discriminazione

La profilazione mediante algoritmi si è spesso dimostrata come fonte di discriminazione: gli output del sistema richiedono un'interpretazione (la quale si concretizza nel comportamento da seguire in base alle indicazioni dell'algoritmo) e per i dati comportamentali, le correlazioni "oggettive" possono arrivare a riflettere «le motivazioni inconsce, le particolari emozioni, le scelte deliberate, le determinazioni socio-economiche, le influenze geografiche o demografiche[68]». In particolare eventuali bias possono derivare da diversi fattori: da errori o decisioni progettuali, da dati parziali[69], ovvero da pregiudizi sociali involontari, quali riflesso di più ampi valori culturali o organizzativi[70]. In ogni caso, gli algoritmi di machine learning, creati a partire da dati viziati, imparano inavvertitamente a riflettere i pregiudizi sottesi alle informazioni elaborate, i quali confluiscono negli output e nei modelli prodotti che possono, quindi, rivelarsi sleali e discriminatori. Così, l'analisi predittiva può contribuire all'autoavveramento

[65] Cfr. Z. ZARSKY, *Transparent Predictions*, 1553–1568. (sostiene la necessità di forti protezioni processuali per compensare la difficoltà di rendere trasparente l'algoritmo predittivo); D.K. CITRON, *Technological Due Process,* in *Washington Univeristy Law Review,* 2008.

[66] I servizi di polizia dovrebbero comunicare al pubblico quali sistemi predittivi utilizzano, in base a quali criteri li hanno scelti e come li valutano. Inoltre, ogni autorità preposta all'applicazione della legge deve consentire alle persone che denunciano comportamenti scorretti della polizia o agli imputati di accedere alla documentazione relativa ai fermi, adottare misure specifiche per impedire l'accesso non autorizzato o il rilascio di dati e rispettare le leggi sulla divulgazione al pubblico dello Stato.

[67] A.G. FERGUSON., *Predictive Policing and Reasonable Suspicion, cit., 324, disponibile a questo indirizzo* digitalcommons.wcl.american.edu (10/06/2020).

[68] M. HILDEBRANDT, (2011) *Who needs stories if you can get the data? ISPs in the era of big number crunching*, in *Philosophy& Technology*, 2011, 376; C. O'NEIL, *op.cit*, 95 ss.

[69] Alcuni reati -come l'omicidio, il furto con scasso e il furto d'auto- tendono ad essere frequentemente denunciati, mentre altri -come la violenza sessuale, la violenza domestica e la frode– tendono a non essere riportati alle autorità. Ad esempio nel 2016, «U.S. residents age 12 or older experienced 5.7 million violent victimizations. » La maggioranza di tali crimini, circa il 58%, non è mai stata denunciata alla polizia. www.bjs.gov; V anche: ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime_statistics (07/04/2020).

[70] B. FRIEDMAN, H. NISSENBAUM, *op. cit.,* 20 ss.

delle profezie e alla stigmatizzazione di gruppi mirati[71]: quando un algoritmo determina se un quartiere è una "zona ad alta criminalità", si avrà un'interpretazione distorta della frequenza dei crimini in aree diverse da quella segnalata come hot spot. Questo porta a concentrare l'intervento delle forze dell'ordine in alcune zone piuttosto che altrove, e man mano che sempre più persone sono fermate, perquisite, arrestate ed eventualmente condannate in quelle aree[72], si contribuisce al verificarsi del c.d. *ratchet effect*[73]. Inoltre, a condurre verso pratiche discriminatorie non sono solo i dati in sé considerati ma anche il modo in cui questi vengono raccolti. Le tecnologie utilizzate per la raccolta delle informazioni sono le più varie, dall'analisi dei social network alle tecnologie di riconoscimento facciale, le quali, più nello specifico, oltre a suscitare perplessità in tema di privacy dei cittadini, hanno sollevato un acceso dibattito sul fronte della loro potenzialità discriminatoria. Sono queste, infatti, le ragioni che hanno portato alla recente ordinanza municipale di San Francisco[74] che vieta l'uso della tecnologia di riconoscimento facciale da parte delle agenzie cittadine e della contea che ha ricevuto l'attenzione internazionale. San Francisco, a lungo al centro della rivoluzione tecnologica, ha preso posizione contro i potenziali abusi vietando l'uso di software di riconoscimento facciale: le preoccupazioni che hanno motivato il divieto sono radicate non solo nella potenziale inesattezza della tecnologia[75], ma anche in

[71] V. C. O'NEIL, *op. cit*., 89: «This creates a pernicious feedback loop. The policing itself spawns new data, which justifies more policing. And our prisons fill up with hundreds of thousands of people found guilty of victimless crimes. Most of them come from impoverished neighborhoods, and most are black or Hispanic. So even if a model is color blind, the result of it is anything but. In our largely segregated cities, geography is a highly effective proxy for race».

[72] Obiezioni , queste, che possono essere superate solo qualora gli algoritmi e i software utilizzati per l'analisi dei grandi dati siano resi più trasparenti, in modo che sia possibile valutare i processi sottostanti e gli standard utilizzati.

[73] B. FRIEDMAN, H. NISSENBAUM, *op. cit*., 28: «And the fact is, given the paucity of reliable information on natural offending rates, law enforcement relies heavily on arrest, conviction, and supervision data in deciding how to allocate resources. This, in turn, accelerates the imbalance in the prison population and acts like a ratchet.[...] Instead of sampling randomly—which would net a proportional representation of the offending population—we are sampling in greater numbers from the pool of higher offenders, and thereby skewing our sample results. Somewhat counter-intuitively, the only way to produce a prison population that mirrors the offending population is to sample randomly from the general population—to engage in essentially random searches, or random audits, or random policing. […] What the ratchet effect does is to disproportionately distribute criminal records and criminal justice contacts with terrible effects on the profiled population»; v. anche B.E. HARCOURT, *Against prediction: profiling, policing, and punishing in an actual age,* in *University of Chicago Press*, 2006, 145 ss.

[74] Stop Secret Surveillance Ordinance n.190110, 05/06/2019.

[75] Studi recenti hanno dimostrato che i sistemi di riconoscimento facciale sono imprecisi nell'identificare le minoranze razziali, le donne e le persone trans gender. Vedi T. SIMONITE, *Photo algorithms ID white men fine-Black Women not so much*, in *Wired*, 2018; J. BUOLAMWINI, *How I'm fighting bias in algorithms*, in *Algorithmic Justice League*, 2016. Video disponibile all'indirizzo www.ajlunited.org (07/04/2020): Joe Buolamwini, tra gli altri ricercatori che hanno testato le caratteristiche dei servizi di analisi facciale di Microsoft e IBM che dovrebbero identificare il genere delle persone nelle foto, evidenzia come gli algoritmi delle aziende si sono dimostrati quasi perfetti nell'identificare gli uomini con la pelle più chiara, ma spesso hanno commesso errori nell'analizzare immagini di donne con pelle scura; J. BUOLAMWINI, T. GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research, 81, 2018, proceedings.mlr.press (07/04/2020); O. KEYES, *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition*, in *ACM Digital Library*, 2018.

una lunga storia nazionale di sorveglianza statale politicizzata e razzista[76]. Il divieto, ha sollevato le polemiche di coloro – principalmente lobbisti aziendali[77] e rappresentanti delle forze dell'ordine[78] – che si oppongono all'ordinanza in nome della "pubblica sicurezza" sostenendo che, poiché l'apprendimento automatico diventa sempre più accurato, la tecnologia in futuro arriverà a eliminare il problema della discriminazione. Anche considerando miglioramenti nell'accuratezza, i difensori dei diritti civili e i ricercatori avvertono che in assenza di una supervisione del governo, la tecnologia potrebbe facilmente essere usata in modo improprio, danneggiando sproporzionatamente le persone già storicamente soggette a profilazione e abusi, tra cui ex detenuti, gli attivisti politici, immigrati e le minoranze etniche[79]. Ignorare l'involontario pregiudizio negli algoritmi di apprendimento automatico pone un rischio particolarmente insidioso per i gruppi svantaggiati creando una giustificazione pseudo scientifica per un trattamento discriminatorio, esentando questi metodi da valutazioni critiche[80]. Un esempio del collegamento tra le pratiche di polizia illegali e distorte e i dati disponibili per implementare i sistemi di polizia predittiva è rappresentato dal caso di New Orleans: il Dipartimento di giustizia ha indagato due volte sul Dipartimento di polizia di New Orleans (NOPD). La prima indagine – che si concentrava su una vasta gamma di comportamenti scorretti delle forze dell'ordine si è conclusa senza un decreto di consenso, a fronte del solo impegno del NOPD si a riformarsi[81]. Tuttavia, nel 2010, su invito del sindaco della città, il Dipartimento ha riaperto la sua indagine esaminando i registri tra il 2005 e il 2011. I risultati evidenziavano come le politiche adottate dal NOPD fossero discriminatorie sulla base della

[76] A. MAK, Facing Facts- A case in Florida demonstrates the problems with using facial recognition to identify suspects in low-stakes crimes, in Slate, 2019; www.aclunc.org (07/04/2020).

[77] Z. DOFFMAN, *San Francisco bans facial recognition as fearmongering trumps common sense*, in *Forbes*, 2019

[78] K.J. DEL GRECO, *Law Enforcement's Use of Facial Recognition Technology, Statement Before the House Committee on Oversight and Government Reform*, FBI, 2017. www.fbi.gov (09/04/2020); Il capo della polizia di Oakland, Anne Kirkpatrick, ha detto in un rapporto indirizzato al consiglio comunale che la tecnologia di riconoscimento facciale può permettere alla polizia di accelerare il «lungo processo manuale di collegamento delle immagini dalle scene del crimine ai database locali delle foto segnaletiche». Invece di vietare la tecnologia, il dipartimento suggerisce di vietare solo la tecnologia di riconoscimento facciale in tempo reale per inviare un messaggio sulle preoccupazioni che circondano la tecnologia, lasciando la porta aperta per il suo eventuale utilizzo. A.E. KIRKPATRICK, *Facial Recognition Ordinance Amendment - Supplemental Report,* 17/06/2019.

[79] Una proposta circa l'uso della tecnologia di riconoscimento facciale, volta ad evitare pericolosi automatismi e abusi, è quella di Daniel Castro, direttore del Center for Data Innovation della Information Technology and Innovation Foundation, il quale suggerisce di sottoporre l'accesso, da parte della polizia, ai dati di riconoscimento facciale solo previo mandato di un giudice, seguendo le linee guida che la Corte Suprema ha stabilito per altre forme di sorveglianza elettronica (quali, ad esempio, per il tracciamento GPS). K. CONGER, R. FAUSSET, S.F. KOVALESKI, *San Francisco Bans Facial Recognition Technology, in The New York Times,* 2019.

[80] S. BAROCAS, A.D. SELBST, *Big Data's Disparate Impact*, in *California Law Review*, 2016. Disponibile in SSRN: papers.ssrn.com (09/04/2020): «Because the discrimination at issue is unintentional, even honest attempts to certify the absence of prejudice on the part of those involved in the data mining process may wrongly confer the imprimatur of impartiality on the resulting decisions. Furthermore, because the mechanism through which data mining may disadvantage protected classes is less obvious in cases of unintentional discrimination, the injustice may be harder to identify and address»; B. CUSTERS, T. CALDERS, B.SCHERMER, T.ZARSKY, *Discrimation and Privacy in the information society. Data mining and profiling in large databases*, Berlino, Heidelberg, 2013.

[81] A. JOHNSON JR., *What the Studies Said,* in *New Orleans Magazine,* 2011, www.myneworleans.com (11/05/2020). In particolare viene ditto che «The federal government delayed their "takeover" and gave the opportunity to reform itself» over the next decade. «Last week the Department of Justice gave the NOPD a "vote of confidence" in how the department was managed and how its officers treat citizens».

razza[82], dell'origine nazionale, e dello status LGBT[83]. Così, al fine di rendere più neutrale il lavoro delle forze dell'ordine, e di ridurre gli eventi criminosi nella città, nel 2012 il NOPD ha avviato una *partnership* con Palantir[84]. Al di là della mancanza di trasparenza della collaborazione[85] – che ha portato all'annullamento dell'accordo nel 2018 – ciò che è interessante rilevare è che, lungi dal correggere le pratiche illecite registrate in capo al dipartimento di polizia, il sistema associava i reati violenti o di gruppo a «giovani, afro-americani, maschi, sotto educati e sottoccupati», ovvero la stessa fetta di popolazione impropriamente presa di mira dalle pratiche del NOPD[86]. Ciò dimostra che quando i dati sporchi sono inseriti in un sistema predittivo, che dovrebbe essere "neutro", questo può essere facilmente contaminato da tali dati nonché dai pregiudizi radicati nelle condotte della polizia. Questo in particolare qualora manchi un'autorità indipendente in grado di controllare le attività dei dipartimenti di polizia così come la raccolta, l'analisi e l'uso dei dati al fine di applicare restrizioni o divieti sull'uso dei dati

[82] Infatti, nel 2009 i dati sull'arresto forniti dal NOPD indicano che, contro la detenzione di 500 maschi afro-americani di età inferiore ai 17 anni, solo otto maschi bianchi della stessa età sono stati presi in custodia. La stessa situazione è stata vissuta dalle donne di questa stessa fascia d'età. In termini di tassi di arresto, sia per i maschi afro-americani ai maschi bianchi, sia per le femmine afro-americane alle femmine bianche, era quasi 16 a 1. U.S. Department of Justice Civil Rights Division, *Investigation of the New Orleans Police Department*, 2011, ix. www.justice.gov (09/04/2020).

[83] Più dettagliatamente sul punto: «We find reasonable cause to believe that there is a pattern or practice of unconstitutional conduct and/or violations of federal law with respect to discriminatory policing. NOPD personnel at all levels of the Department not only acknowledged that the community perceives racial and ethnic profiling as a significant problem, but some also expressed their own belief that such discriminatory conduct occurs. Both bias and the perception of bias erode citizens' inclination to trust and cooperate with law enforcement, impeding effective and safe policing. Although both community members and officers told us that this dynamic is clearly at work in New Orleans, the Department has failed to respond with systems to prevent, detect, and respond to discriminatory policing, and to ensure that police officers are conducting themselves in accordance with constitutional guarantees of equal protection. The Department's inadequate policies and training in conducting proper stops, searches, and arrests increase the likelihood that officers, without sufficient understanding of how to identify and articulate suspicion based on behavior and other permissible factors, will instead rely on inappropriate stereotypes and bias in their decision-making». *U.S. Department of Justice Civil Rights Division, Investigation of the New Orleans Police Department*, 2011. www.justice.gov (09/04/2020).

[84] «Palantir Law Enforcement features an intuitive, user-friendly interface that allows any agent, detective, or investigator to quickly access all available information in one place. Instead of logging in to separate systems, users can conduct one search for a suspect, target, or location through a single portal and return data from all relevant systems. Palantir Law Enforcement supports existing case management systems, evidence management systems, arrest records, warrant data, subpoenaed data, RMS or other crime-reporting data, Computer Aided Dispatch (CAD) data, federal repositories, gang intelligence, suspicious activity reports, Automated License Plate Reader (ALPR) data, and unstructured data such as document repositories and emails». www.palantir.com (09/04/2020)

[85] Infatti, il programma è sfuggito all'attenzione del pubblico, in parte perché Palantir lo ha stabilito come rapporto filantropico con la città attraverso il programma NOLA For Life, firmato dal sindaco Mitch Landrieu. Grazie al suo status filantropico, così come al modello di governo del "forte sindaco" di New Orleans, l'accordo non è mai passato attraverso una procedura di appalto pubblico. www.theverge.com (10/04/2020)

[86] S. SHIRMER, *Deploying Palantir Gotham in New Orleans, 2014.* assets.documentcloud.org (10/04/2020); Vedi anche: A. WINSTON, *Palantir has secretly been using New Orleans to test its predictive policing technology,* in *Verge, 2018. www.theverge.com* (10/04/2020); Palantir Techs., *NOLA murder reduction: technology to strategies*, 2014. www.documentcloud.org (10/04/2020): descrive il partenariato tra Palantir e la città di New Orleans per identificare «individuals exhibiting the highest predictors of violence».

storici generati da pratiche illegali e di parte così da evitare il perpetuarsi di tali pratiche attraverso sistemi automatizzi.

4. Considerazioni conclusive

Gli ultimi vent'anni hanno visto un notevole aumento di politiche e pratiche basate sui dati nel settore pubblico, al fine di ridurre la dipendenza da fattori soggettivi e di reagire in modo più oggettivo alle questioni sociali, economiche e politiche. Tuttavia, la crescente dipendenza dai dati presenta seri rischi per l'equità e la giustizia, in mancanza di un attento monitoraggio alla base della creazione, della revisione e del mantenimento dei dati stessi. Se, da un lato, i *Big Data* e l'analisi predittiva sono uno strumento molto utile per la repressione dei reati, dall'altro, emerge la necessità di trovare un equilibrio tra l'efficace applicazione della legge (e la prevenzione del crimine) e i diritti dell'individuo[87].
In primo luogo, poiché la legge sulla privacy non è stata, finora, in grado di affrontare il concetto di «thousands of small acts of data gathering – each individually unharmful, authorized by the user, or gathered by different parties – may in their total, quantitative volume create a privacy violation[88]», una nuova nozione di "privacy quantitativa" potrebbe essere presa in considerazione, tenuto conto dello sviluppo delle nuove tecnologie e dei "grandi dati". Ecco perché, da più parti, si ritiene necessaria una normativa specifica per questa particolare tecnica investigativa, nonché la costituzione di un'autorità indipendente che controlli, in primo luogo, l'acquisizione delle informazioni, ne autorizzi l'uso e verifichi, a lungo termine, le operazioni di polizia[89]. Inoltre, ove opportuno, tale autorità dovrebbe poter imporre sanzioni nel caso in cui le norme di legge non siano rispettate o qualora rilevi pratiche discriminatorie, o comunque lesive dei diritti costituzionali dell'individuo[90]. Pertanto risulta necessario

[87] Per esempio l'art. 26, comma 1 del nostro Codice della Privacy prevede che il trattamento dei dati sensibili può essere effettuato solo con il consenso scritto dell'interessato e previa autorizzazione del Garante. Tuttavia, al comma 4 dell'art. 26 si precisa che in alcuni casi, come in una delle indagini difensive, i dati sensibili possono essere trattati senza il consenso, ma con l'autorizzazione del Garante. Inoltre, l'art. 27 precisa che il trattamento di dati giudiziari da parte di privati o enti economici pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichi le relative finalità di interesse pubblico del trattamento, le tipologie di dati trattati e le operazioni eseguibili.

[88] K. MILLER, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, in *Journal Technology of Law and Policy*, 2014, 105-127.

[89] Tale esame dovrebbe cercare di fare una selezione dei Dati che potrebbero essere registrati e successivamente utilizzati dal software, questo perché è impossibile distinguere tra politiche o pratiche problematiche potenziali ed effettive: una valutazione di questo tipo può essere fatta solo nel lungo periodo. Per autorità indipendenti si intendono quegli enti o enti pubblici, istituiti dalla legge, che esercitano funzioni prevalentemente amministrative in aree ritenute sensibili o di elevato contenuto tecnico (concorrenza, privacy, comunicazioni, ecc.) tali da richiedere una particolare posizione di autonomia e indipendenza nei confronti del Governo, al fine di garantire una maggiore imparzialità (cd. neutralità) rispetto agli interessi coinvolti. V. G. FALCON, *Lezioni di diritto amministrativo*, Padova, 2016. Sull'indipendenza si veda G. NAPOLITANO, *Autorità indipendenti e agenzie amministrative*, in M. CLARICH, G. FONDERICO (a cura di), *Dizionario di diritto amministrativo*, *Il Sole 24 Ore*, 2007, 87 ss.; R. CHIEPPA, G.P. CIRILLO, *Le autorità amministrative indipendenti*, Padova, 2010, 38.

[90] Un altro esempio di pratiche discriminatorie è dimostrato da un'indagine ProPublica del 2016 sul software di polizia predittiva, che dimostra che gli algoritmi offender-based erano portati a identificare erroneamente gli imputati neri come soggetti ad alto rischio e, al contrario quelli bianchi come individui a basso rischio. J. ANGWIN,

elaborare misure tecniche in grado di garantire piena responsabilità e trasparenza algoritmica al fine di evitare conseguenze negative per quanto riguarda il diritto alla privacy nonché conseguenze discriminatorie. Solo il rispetto di tali garanzie può eliminare, o almeno ridurre, la conformità delle pratiche di polizia predittiva con la protezione dei diritti civili. Ciò legittimerebbe l'uso, da parte delle forze dell'ordine, di potenti strumenti che indubbiamente contribuiscono alla salvaguardia della sicurezza pubblica[91].

Resta da sottolineare che l'analisi predittiva non è uno strumento limitato a colpire i criminali, potendo essere utilizzato per identificare i bisogni sociali e i problemi economici che coinvolgono quelle aree ad alto tasso di criminalità: questa è la «promise of bright data»[92]. I sistemi di previsione possono funzionare e fornire benefici a diversi livelli: da un lato, faciliterebbero l'azione delle forze dell'ordine nel definire le aree critiche, allocare le risorse nel modo più efficace possibile in ogni momento, intervenire a livello operativo con iniziative volte a prevenire e sradicare i fenomeni criminali e misurare costantemente i risultati raggiunti; dall'altro, aiuterebbe le amministrazioni locali a scoprire la portata dei fenomeni e la loro natura, in modo da poter elaborare politiche e misure più efficaci nel campo della criminalità e della sicurezza pubblica e monitorarne i risultati; infine, fornirebbe ai cittadini un'informazione più specifica e obiettiva sul livello di sicurezza della città e consigli sul miglior comportamento preventivo da adottare.

J. LARSON, S. MATTU, L. KIRCHNER, *Machine Bias. There's software used across the country to predict future criminals. And it's biased against blacks*, in *ProPublica*, 2016.

[91] Il 31 agosto 2016, una coalizione di diciassette organizzazioni ha rilasciato una dichiarazione sugli strumenti di polizia predittiva utilizzati dalle forze dell'ordine negli Stati Uniti, indicando i pregiudizi razziali della tecnologia, la mancanza di trasparenza e altri profondi difetti che portano all'ingiustizia. Cfr. Statement of concern about predictive policing by ACLU and 16 civil right privacy, racial justice, and technology organizations, 2016. www.aclu.org (10/04/2020): «Vendors must provide transparency, and the police and other users of these systems must fully and publicly inform public officials, civil society, community stakeholders, and the broader public on each of these points. […] The Fourth Amendment forbids police from stopping someone without reasonable suspicion — a specific, individualized determination that is more than just a hunch […]Similarly, predictive policing must not be allowed to erode rights of due process and equal protection.[…] Systems that are currently deployed, or are contemplated for future deployment, must each be publicly audited and monitored on an ongoing basis for their disparate impact on different communities the police department serves, with results broken out by race and by neighborhood»; Anche a livello Europeo, si è cercato di indicare alcuni principi e linee guida per l'utilizzo delle nuove tecnologie predittive in ambito giurisdizionale. V. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment*, 3, 12, 2018, 4 e 47.

[92] A.G. FERGUSON, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, in *New York University Press*, 2017, 5-6. Più in generale si vedano le considerazioni di E. STRADELLA, *op. cit*., 10: «Ma soprattutto, quello che forse il diritto potrebbe chiedere in più all'*AI* è di fornire gli strumenti capaci di guidare le decisioni orientandole ai valori del costituzionalismo. Strumenti in grado di rappresentare la realtà senza amplificarne le ingiustizie, ma anzi sfruttando l'infinita possibilità di accuratezza e di completezza che sempre di più caratterizza i dati, e la progressiva espansione della potenza di calcolo, per sradicarle, attraverso algoritmi costruiti come azioni positive».