DIPARTIMENTO DI GIURISPRUDENZA

CATTEDRA DI DIRITTO PENALE

L'INTELLIGENZA ARTIFICIALE NELLE ATTIVITÀ DI LAW ENFORCEMENT

RELATORE

Chiar.mo Prof.

Maurizio Bellacosa

CORRELATORE

Chiar.mo Prof.

Mitja Gialuz

CANDIDATA

Ginevra Sabia

Matr. 159063

ANNO ACCADEMICO 2022/2023

L'INTELLIGENZA ARTIFICIALE NELLE ATTIVITÀ DI LAW ENFORCEMENT

INTRODUZIONE

CAPITOLO I

I BIG DATA, ALGORITMI E NUOVE TECNOLOGIE DI APPRENDIMENTO

1. Cosa sono I *BIG DATA*?

1.2 Gli strumenti utilizzati per monitorare i *big data*

2. La classificazione dei big data: i *black data*, i *blue data*, i *bright data*

2.1 I *Black data*

2.2 I *Blue data*

2.3 I *Bright data*

3. I Metadati

4. Il procedimento di acquisizione dei dati

5. La problematica della mancanza di dati

6. La fallibilità dei dati

7. La sistematica degli algoritmi predittivi

7.1 Strategie e tecniche dell'accusa basata su algoritmi: l'esperienza statunitense

8. Il *machine learning* e le sue potenzialità in campo penale

CAPITOLO II

PREDICTIVE POLICING

1. Nozioni preliminari: cosa si intende per ''*predictive policing*''?

1.1 Dal sospetto al crimine

CAPITOLO III

LA TECNOLOGIA DEL RICONOSCIMENTO FACCIALE

INTRODUZIONE

L'intelligenza artificiale (*AI*, *Artificial intelligence*) può essere definita come un sistema tecnologico attraverso il quale, le macchine, grazie ad appositi *software*

avanzati, simulano i processi dell'intelligenza umana. Il grande avanzamento tecnologico, che aumenta di giorno in giorno, sta, per questo, stravolgendo il rapporto uomo-macchina. Queste ultime, infatti, non sono più mere esecutrici di *input* umani, ma sono in grado di elaborare *output* completamente autonomi dalle informazioni immesse nel linguaggio di programmazione e, per questo, sfuggono sempre di più al controllo umano. Per questi motivi l'IA è un tema centrale nel dibattito nazionale e internazionale, in relazione alle potenzialità e ai rischi correlati al suo uso frequente.

La vera rivoluzione, relativamente al tema in esame, nasce dal fatto che questi nuovi sistemi intelligenti riescono compiere innumerevoli azioni in tempi molto più rapidi rispetto all'uomo e, spesso, con maggiore efficienza, sono in grado di prendere decisioni, imparare dagli errori ed elaborare ragionamenti complessi propri. Grazie a queste caratteristiche e potenzialità, i *software* basati sull'intelligenza artificiale hanno trovato ampia applicazione in ogni campo.

Infatti, l'intelligenza artificiale è stata adottata, per la sua indubbia utilità, anche nell'ambito della giustizia, dove viene impiegata per agevolare lo svolgimento di alcune attività procedurali tra cui, per quello che qui interessa, aiutare le forze di polizia nelle operazioni di prevenzione e repressione del crimine.

Tali finalità stravolgono completamente il tradizionale sistema della giustizia, ragion per cui, si è posta la necessità, sollecitata dagli studiosi del diritto e dai giuristi, di meglio regolare il tema, mediante una normativa *ad hoc*, di incrementare controlli e correttivi relativi all'uso dell'IA relativamente alla sua applicazione pratica nel settore giudiziario, in particolare quello penale. L'uso incontrollato di questi sistemi, senza limiti imposti dalla legge, rischia, infatti, come è già accaduto in altre giurisdizioni come ad esempio negli Stati Uniti, rischia di tradursi in veri sistemi di controllo di massa che limitano irrimediabilmente e in modo improprio le libertà individuali e violano i diritti fondamentali costituzionalmente sanciti. Per questo si rende necessaria, come detto, una regolamentazione normativa specifica, onde evitare che le scienze di IA vengano utilizzate in maniera irresponsabile e inconsapevole, cagionando gravi implicazioni di ordine tecnico-giuridico ed etico. Lo scopo del diritto è quello di ricercare un equilibrio normativo che impedisca alle nuove tecnologie di violare diritti fondamentali dell'individuo.

Da queste considerazioni di fondo, che esaminano il tema dei rapporti tra Intelligenza artificiale e sistema penale, e in generale tra macchina-uomo, è nato l'interesse all'elaborazione del presente elaborato, nel quale, si è cercato di esaminare come l'IA abbia causato una vera rivoluzione nelle attività di *law enforcement*, foriera, oltre che di oggettivi benefici, di indiscutibili perplessità ed incertezze.

Infatti, con il crescente utilizzo di algoritmi predittivi, volti a prevenire la criminalità, unitamente alla diffusione di macchine intelligenti, si è assistito a una modifica dei processi decisionali, che a differenza del passato, non derivano più esclusivamente della valutazione e apprezzamento dell'uomo. Tecnicamente, il sistema penale che si prospetta svilupparsi nel mondo, si basa sulla prevenzione della criminalità mediante l'utilizzo di algoritmi, sistemi in grado di raccogliere ed elaborare grosse quantità di informazioni (i c.d. "*big data*", che rappresentano la base delle tecnologie predittive).

Essi sono utilizzati per prevenire reati, individuando i luoghi a rischio di criminalità (*crime hotspot*) o per elaborare profili criminali personalizzati di individui a rischio di delinquenza. Tali algoritmi sono finalizzati per l'appunto alla diminuzione del tasso di criminalità (anche se i dati statistici in merito sono discordanti circa il livello effettivo di riduzione) e alla precisione delle analisi di informazioni investigative. La capacità, infatti, di studiare e confrontare ingentissime quantità di dati in pochissimo tempo è assolutamente vantaggiosa per l'uomo, il quale non potrebbe competere con le macchine nel gestire simili quantità di informazioni.

Tralasciando le indubbie utilità descritte, è altrettanto vero che l'incisiva attività di monitoraggio svolta attraverso la raccolta di una mole di dati personali così elevata, in maniera quasi "selvaggia" e spesso all'insaputa del cittadino, può violare o limitare i diritti fondamentali, primo fra tutti la sua *privacy* e, può creare possibili discriminazioni qualora gli indici di pericolosità di un individuo siano condizionati da pregiudizi (*bias*).

Una seconda applicazione, frutto dell'impiego dell'IA nelle attività di *law enforcement*, è rappresentata dalle tecniche di riconoscimento facciale, che pure saranno oggetto della nostra analisi, con riferimento specifico a tutte le limitazioni e violazioni dei diritti che derivano dal loro utilizzo.

Completato l'esame di queste due importanti tecnologie – *predictive policing* e *facial recognition* – ci confronteremo infine, con l'impatto degli algoritmi sui diritti fondamentali dell'individuo.

CAPITOLO I

I *BIG DATA*, ALGORITMI E NUOVE TECNOLOGIE DI APPRENDIMENTO

1.Cosa sono I *BIG DATA*?

Al giorno d'oggi tutti sono controllati[1], il mondo è interconnesso da un'unica rete digitale, tutti sono sorvegliati, spiati, tutti sono il prodotto di un grandissimo marketing in cui il prezzo sono i dati, la *privacy*.

I *big data* sono al centro di questo sistema di controllo, ma cosa sono? In generale con tale termine ci si riferisce ai processi di raccolta e analisi di grandi quantità di dati, o di informazioni, messi insieme con l'obiettivo di rivelare modelli o caratteristiche soggettive nascoste[2]''.

Un rapporto dell'Ufficio Esecutivo del Presidente degli Stati Uniti ha riassunto che nonostante ci siano molte definizioni di *big data*, la maggior parte di esse riflette la capacità tecnologica di acquisire, aggregare, elaborare un volume, una velocità, una varietà di dati sempre più grande[3]. In altre parole, grandi raccolte di dati vengono ordinate e riunite da potenti computer che visualizzano le connessioni e le correlazioni – all'occhio umano impercettibili –tra loro[4]; si tratta degli strumenti di *machine-learning*, più precisamente di apprendimento automatico e analisi predittiva[5].

Un esempio sul funzionamento dei *big data* può essere quello di Amazon.com: il sito infatti è in grado di suggerire oggetti che potrebbero interessare al compratore sulla base di ciò che ha già acquistato in precedenza o oggetti che spesso vengono acquistati insieme sulla base di indagini conoscitive su larga scala. Il sito, infatti, collega le transazioni effettuate nel passato con eventuali transazioni future, sulla base degli interessi dei compratori; in sostanza Amazon.com riesce a ''predire'' quali articoli potrebbero essere voluti da quell'utente per il futuro[6].

Sulla base di questo esempio è possibile affermare che i *big data* dimostrano le correlazioni tra singoli dati, creando così una mappatura di

---

[1]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 7.

[2]Cfr., COHEN Julie E., *What Is Privacy For?,* in *HARV,* 2013, 1904-1920-1921, 126.

[3]Cfr., Exec. Office of the President, *Big data: seizing opportunities, preserving values*, 2014, 2 *www.whitehouse.gov*.

[4]Cfr., BERMAN Jules J., *Principles of big data: preparing, sharing, and analyzing complex information,* 2013, 2.

[5]Cfr., LOHR Steve, Amid the Flood, *A Catchphrase Is Born*, in *N.Y. TIMES*, 2012.

[6]Cfr., WOHLSON Marcus, *Amazon's Next Big Business Is Selling You*, in *WIRED*, 2012.

interessi, attitudini di un soggetto o di grandi quantità di individui, offrendo quindi una realtà tanto utile quanto pericolosa.

Secondo la giornalista Julia Angwin ''Stiamo vivendo in una *Dragnet Nation*, un mondo di tracciamento indiscriminato in cui le istituzioni stanno accumulando dati sugli individui ad un ritmo senza precedenti''[7], si tratta quasi di un mondo ''distopico'' sulle righe di 1984 di George Orwell dove tutti sono spiati ''*Big brother is watching you*[8]''.

Per altro verso, il World Privacy Forum, un gruppo di controllo sulla *privacy*, stima che ci siano circa quattromila *database* diversi che raccolgono informazioni sugli individui[9], infatti, ogni volta che si interagisce con un computer, uno *smartphone*, con carte di credito e molto altro, viene lasciata una ''traccia digitale'' che è rivelatrice di informazioni personali e preziose per la *privacy*[10][11].

È possibile, quindi, affermare con certezza che i *big data* provengono dagli individui. Si pensi ad esempio all'indirizzo o al codice postale, questi elementi sono in grado di definire dati demografici ed economici. Negli Stati uniti addirittura il sistema postale gestisce il programma di controllo e tracciamento, fotografando ogni singola posta elaborata e confrontandola con i vari indirizzi; in questo modo anche la posta diventa rivelatrice di dati personali[12]. Le *mail* rivelano dati sugli amici, sui collaboratori, o ancora gli acquisti rivelano gli interessi[13]; l'*iPhone* è in grado di conoscere una vastissima gamma di informazioni sul proprietario, incluso dove va o addirittura in quale clinica sanitaria si è recato[14]; l'automobile se è ibrida o meno può rivelare lo stile di

---

[7]Cfr., ANGWIN Julia, *Dragnet nation: a quest for privacy, security, and freedom in a world of relentless surveillance*, 2014, 3.

[8]Cfr., ORWELL George, *Nineteen Eighty-Four*, Londra, 1949

[9]Cfr., WEISBAUM Herb, *Big Data Knows You're Pregnant (and That's Not All)*, in *CNBC*, 2014, *www.cnbc.com*.

[10]Cfr., CUKIER Kenneth, *Data, Data Everywhere*, in *ECONOMIST*, 2010.

[11]Cfr., FERGUSON, Andrew Guthrie. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. in *Nyu Press*, 2017, 7 s.

[12]Cfr., NIXON Ron, *U.S. Postal Service Logging All Mail for Law Enforcement*, in *N.Y.TIMES* , 2013.

[13]Cfr., STRAHILEVITZ Lior Jacob, Reputation Nation: *Law in an Era of Ubiquitous Personal Information*, in *NW. U.*, 2008, 1667-1720, 102; R. SLOBOGIN Christopher, *Transactional Surveillance by the Government*, in *MISS*, 2005, 139-145, 75.

[14]Cfr., CITRON Danielle Keats, *Spying Inc.*, in *WASH. & LEE*, 2015, 1243-1272, 72.

vita o la visione sul mondo ambientale; il *GPS* monitora la posizione dell'auto e, attraverso programmi come *GM OnStar*, consente aiuto immediato in caso di incidente o emergenza ma lo fa avendo sempre la posizione in tempo reale[15]; come anche i sistemi che fotografano le targhe o più di tutto il tema problematico del riconoscimento facciale.

Tutti questi dati, da soli insignificanti, se messi insieme creano un vero e proprio schema della personalità. L'auto-sorveglianza (poiché i dati provengono dai cittadini) fornisce così la valuta per il profitto commerciale, nonché uno degli elementi costitutivi di uno Stato basato su una polizia invadente in cui gli indizi digitali diventano rilevanti anche per i processi, rivelando segreti spesso tenuti nascosti, lesivi della *privacy*[16].

Dopo aver definito cosa sono i *big data* e da chi derivano queste informazioni, la domanda che ne consegue è: chi possiede i *big data*?

Alcuni soggetti privati, in particolare i *broker* privati, raccolgono, acquistano e vendono dati personali a società interessate a vendere prodotti, determinare il rischio di credito finanziario[17], o addirittura alle forze dell'ordine per condurre le indagini procedurali[18].

La Commissione per il Commercio del Senato degli Stati Uniti ha dettagliato come le società di *big data* come *Acxiom* affermano di avere informazioni su oltre settecento milioni di consumatori in tutto il mondo con oltre tremila segmenti di dati per quasi tutti i consumatori statunitensi[19]. Il rapporto del Senato degli Stati Uniti ha specificato come "un'azienda raccoglie dati sul fatto che i consumatori soffrano di particolari disturbi, o a proposito del loro stato di famiglia[20]''e "un'altra azienda offre in vendita i dati di una

---

[15]Cfr., POTTER Ned, Privacy Battles: *OnStar Says GM Can Record Car's Use, Even If You Cancel Service*, in *ABC NEWS* , 2011 http://abcnews.go.com.

[16]Cfr., FERGUSON, A. G. *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* in *NYU Press*, 2017, 8 s., https://doi.org/10.2307/j.ctt1pwtb27.4.

[17]Cfr., Trade Fed. Comm'n, *Data brokers: a call for transparency and accountability* i–ii, 2014, available at www.ftc.gov.

[18]*Ibidem.*

[19]Cfr., Trade Fed. Comm'n, *Data brokers: a call for transparency and accountability*, 2014, 8.

[20]Cfr., MAJORITY Staff of S. Comm. on Commerce, Sci., & Transp., Office of Oversight & Investigations, *A review of the data broker industry: collection, use, and sale of consumer data for*

lista di consumatori con uno stato delicato di salute[21]''. Queste aziende, che hanno come oggetto di merce i dati delle persone, li raggruppano in base a dati demografici condivisi, sulla base del reddito o dello stato di famiglia[22]. Ad esempio, uomini e donne single di età superiore ai sessantasei anni, con ''basso livello di istruzione e basso patrimonio netto'', sono classificati come *''Rural Everlasting''*[23], altri single della stessa fascia di età ma con un maggiore reddito sono classificati come *''Urban Scramble''* o *''Mobile Mixers''*[24].

Le società di dati privati vendono regolarmente queste informazioni basate sull'attività dei consumatori ad altri *broker* di dati, scambiando dati quindi espandendo ulteriormente le reti di dati condivisi. I *broker* di dati raccolgono informazioni personali per monitorare gli interessi e le inclinazioni degli individui, non sorprende quindi l'interesse della polizia, specialmente quella predittiva, all'acquisizione di questi dati, spesso rilevanti per le indagini su particolari soggetti imputati o sospettati o a ''rischio di commissione di reati''. Così l'acquisizione di dati digitali diventa sempre più rischiosa per la protezione della *privacy* degli individui, che spesso, non essendone a conoscenza, offrono ad una gamma di soggetti indeterminati, informazioni private sulla loro vita, informazioni che potenzialmente potrebbero arrivare a chiunque.

Negli Stati Uniti, addirittura, l'attuale registro della polizia, documento contenente una ingente quantità di dati personali, si trova su un *server cloud* accessibile agli agenti in tutto il Paese[25]. I *database* federali, come il *National Crime Information Center (NCIC),* contengono tredici milioni di documenti, tutti accessibili dagli agenti di polizia, addirittura se un agente di polizia arresta un individuo e ''fa passare il suo nome'' attraverso il sistema, l'*NCIC* è in

---

marketing purposes, 2013, 5 e 8. available at *www.commerce.senate.gov* [hereinafter *A REVIEW OF THE DATA BROKER INDUSTRY*].

[21]*Ibidem.*

[22] Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. in *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, in *NYU Press*, 2017, 9 s., *https://doi.org/10.2307/j.ctt1pwtb27.4*.

[23]Cfr., TRADE Fed. Comm'n, *Data brokers: a call for transparency and accountability* 2014, 20.

[24]*Ivi*, 47.

[25]Cfr., FERGUSON Andrew G. & LOGAN Wayne A., *Policing Criminal Justice Data*, in *MINN.*, 2016, 541- 554, 101.

grado di fornire tutti i suoi dettagli personali, in particolare relativi a eventuali arresti precedenti, mandati, affiliazioni a bande o legami terroristici, *status* di fuggitivo, nonché informazioni sulla proprietà o sul possesso di armi, licenze di auto[26]. Il governo federale mantiene anche elenchi di controllo incentrati sul terrorismo, inclusi settecentomila nomi nel *Terrorist Screening Database (TSD)*, un milione di nomi nel *Terrorist Identities Datamart Environment (TIDE)* e cinquecentomila nomi nella *"No-Fly List"*[27].

Gli Stati Uniti raccolgono e generano anche *set* di dati per monitorare i cittadini. Undici stati mantengono ampi database elettronici, ad esempio, su probabili componenti di una associazione criminale[28], o ancora su individui condannati per reati con armi da fuoco[29], sono presenti anche dettagli su dati personali come la residenza-domicilio dei trasgressori[30], dove lavorano e vanno a scuola se minori. Una vasta gamma di organizzazioni delle forze dell'ordine condividono, quindi, dati personali su sospetti, crimini e modelli di criminalità. Queste organizzazioni includono: agenzie statali, locali e territoriali, il Dipartimento di Giustizia (DOJ), il Dipartimento della Sicurezza Nazionale (DHS), il *Federal Bureau of Investigation (FBI), la Drug Enforcement Administration (DEA)* e il *Bureau of Alcohol, Tobacco, and Firearms (ATF)*[31].

Una rete di centri di fusione, inoltre, condivide le informazioni relative alle minacce attraverso i confini federali e statali[32]. I Centri Regionali di Sistemi di Condivisione delle Informazioni (*Regional Information Sharing Systems-RISS)* coordinano i dati in arrivo, mentre i Centri di Analisi del Crimine (*Crime*

---

[26]Cfr., *US Department of Justice, FBI, Criminal Justice Information Services Division, CJIS ANNUAL REPORT* 4, 2015.

[27] Cfr., LIND Dara, *Turning the No Fly List into the No Gun List Explained*, in *VOX*, 2016, *www.vox.com*; JANSEN Bart, *America's Terrorist Watchlist Explained*, in *USA TODAY*, 2016.

[28]Cfr., HOWELL K. Babe, *Gang Policing: The Post Stop-and-Frisk Justification for Profile-Based Policing,* , in *U.DENV.CRIM* , 2015, 1-15-16, 5.

[29]Cfr., LOGAN Wayne A., *Knowledge as power: criminal registration and community notification laws in America*, 2009, 178 – 81.

[30] Cfr., LOGAN Wayne A., *Database Infamia: Exit from the Sex Offender Registries*, in *WIS*, 2015, 219.

[31]Cfr., FERGUSON A. G., 2017 *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 11 s.

[32]Cfr., CITRON Danielle Keats & PASQUALE Frank, *Network Accountability for the Domestic Intelligence Apparatus*, in *HASTINGS*, 2011, 1441-1451, 62.

Analysis Centers-CACs) analizzano i dati raccolti. Queste nuove entità di condivisione dei dati si coordinano anche con le 17 diverse agenzie che compongono la comunità di *intelligence* degli Stati Uniti, comprese le agenzie di raccolta dati verso l'esterno e rivolte a livello internazionale come la *National Security Agency* (*NSA*) e la *Central Intelligence Agency* (*CIA*)[33]. Progetti sull'acquisizione-analisi di dati come il *National Data Exchange Program (N-DEx)* sono stati istituiti "come un gigantesco *data warehouse*" per mettere insieme i vari database della polizia[34].

Come evidenziato nella "Valutazione dell'impatto sulla privacy" di N-DEx: *''N-DEx* fornisce un sistema nazionale di condivisione delle informazioni investigative disponibile attraverso un sito Internet sicuro che consente alle agenzie che si occupano di giustizia criminale, un archivio di informazioni, da poter ricercare e analizzare, proveniente da entità locali, statali, regionali, e federali, *N-DEx* fornisce a queste agenzie la capacità di creare collegamenti tra incidenti criminali, indagini penali ed eventi correlati per aiutare a risolvere, scoraggiare e prevenire i crimini[35]. . . *N-DEx* contiene le informazioni di identificazione personale (PII) di sospetti, autori, testimoni e vittime e chiunque altro possa essere identificato in un rapporto delle forze dell'ordine riguardante un incidente criminale o un'indagine penale[36]''.

A partire dal 2014, *N-DEx* aveva oltre 107.000 utenti e oltre 170 milioni di informazioni ricercabili[37].

Alcune *start-up* hanno costruito, altresì, sistemi di gestione dei dati a supporto delle attività di *law enforcement*.

Le forze dell'ordine, negli Stati Uniti, oltre a collezionare dati all'interno dei registri investigativi, ora raccolgono anche dati biologici, in particolare dati biometrici.

---

[33]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York, 2017, 12.

[34]Cfr., MITCHELL Robert L., *It's Criminal: Why Data Sharing Lags among Law Enforcement Agencies*, in *COMPUTER WORLD*, 2013, *www.computerworld.com.*

[35]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York, 2017, 13 s.

[36]Cfr., N-DEX, *Privacy impact assessment for the national data exchange* in (*N-DEX) SYSTEM*, 2014, available at *www.fbi.gov*.

[37]*Ibidem.*

La raccolta biometrica include dati sul DNA, impronte digitali, fotografie e scansioni dell'iride e della retina, il tutto protetto in *database* consultabili per indagare su taluni crimini[38]. Rientrano tra tali database: il *Combined DNA Index System (CODIS)*che include 12 milioni di profili di DNA ricercabili[39], il sistema *Next Generation Identification (NGI)* dell'FBI che registra impronte digitali, impronte dei palmi, riconoscimento facciale. L'FBI ha, così, oltre 23milioni di fotografie ricercabili avendo la più grande collezione di impronte digitali al mondo[40].

Tutti questi dati spingono le indagini della polizia nel futuro, e tutto ciò apre l'opportunità a nuovi strumenti di *big data* per ordinare, cercare e scoprire connessioni altrimenti nascoste tra crimine e criminali; è una vera e propria rivoluzione per le indagini[41].

I professionisti dell'analisi dei dati, spesso privati, partecipano abitualmente a sessioni di strategia nei grandi dipartimenti di polizia[42], che addirittura posseggono un direttore per l'analisi dei dati[43].

Essendo l'acquisizione dei *big data* un tema problematico nella prassi, molte leggi federali sulla privacy limitano la raccolta governativa diretta a informazioni personali; tra queste rientrano: il *Privacy Act* del 1974[44], l'*Electronic Communications Privacy Act* del 1986 *(ECPA)*[45], lo *Stored*

[38]Cfr., HU Margaret, *Biometric ID Cybersurveillance*, in *IND*, 2013, 1475-1478, 88; DONOHUE Laura K., *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, in *MINN.*, 2012, 407-435, 97; MURPHY Erin, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, in *CAL* 2007, 721-728, 95.

[39]Cfr., *FBI,CODIS NDIS STATISTICS* , 2016, *www.fbi.gov*.

[40]Cfr., *U.S. Dep't of Justice, FBI, Criminal Information Services Division, NEXT GENERATION IDENTIFICATION FACTSHEET*, 2016, *www.fbi.gov*.

[41]Cfr., FERGUSON Andrew Guthrie, *Big Data and Predictive Reasonable Suspicion*, in *U.PA.*, 2015, 327-370, 163; JOH Elizabeth E., *Policing by Numbers: Big Data and the Fourth Amendment*, in *WASH.* , 2014, 35-42, 89; FERGUSON Andrew Guthrie, *Predictive Policing and Reasonable Suspicion*, in *EMORY*, 2012, 259-266, 62.

[42]Cfr., MYERS Laura, PARRISH Allen & WILLIAMS Alexis, *Big Data and the Fourth Amendment: Reducing Overreliance on the Objectivity of Predictive Policing*, in *CTS* , 2015, 231-234, 8.

[43]Cfr., CHOHLAS-WOOD Alex *is the current director of analytics at the Office of Management Analysis and Planning, New York Police Department*.

[44]Cfr., 5 U.S.C. § 552a (1994).

[45]Cfr., Pub. L. No. 99–508, 100 Stat. 1848 (sezione 18 U.S.C.); *Communications Assistance for Law Enforcement Act*, Pub. L. No. 103–414, 1994, §207(2).

Communications Act (SCA)[46], il *Foreign Intelligence Surveillance Act (FISA)*[47], l'*E-Government Act* del 2002[48], il *Financial Privacy Act*[49],il *Communications Act, Gramm-Leach-Bliley Act*[50], il *Bank Secrecy Act*[51], il *Right To Financial Privacy Act*, , il *Fair Credit Reporting Act*[52], l'*Health Insurance Portability and Accountability Act* del 1996 *(HIPAA)*[53],il *Genetic Information Non-discrimination Act (GINA)*[54],il *Children's Online Privacy Protection Act (COPPA)*[55], il *Family Educational Rights and Privacy Act*[56],e il *Telephone Records and Privacy Protection*[57]del 2006 insieme al *Video Protection Privacy Act*[58].

Per tutelare la privacy e la riservatezza, la polizia può ottenere determinati dati soltanto con un ordine del tribunale o un mandato di comparizione[59]. Il tema della privacy, tuttavia, resta problematico in quanto non impedisce alle forze dell'ordine di acquistare le informazioni di un determinato individuo su Internet direttamente dalle aziende private che collezionano dati[60],pur non essendosi ancora verificata una completa convergenza tra l'attività di raccolta di *big data* da parte delle aziende private e la raccolta delle forze dell'ordine.

In questo sistema i dati privati finiscono spesso per diventare parte dei registri pubblici, e i registri pubblici, a loro volta, diventano gli elementi costitutivi dei database privati e governativi. I dati vengono venduti e

[46] Cfr., 18 U.S.C.§§ 2701–12.

[47] Cfr., 50 U.S.C.. §§ 1801–13.

[48] Cfr., 44 U.S.C.§§ 3501–21.

[49] Cfr., 12 U.S.C.§§ 35.

[50] Cfr., 15 U.S.C.§ 6801.

[51] Cfr., 12 U.S.C.§§ 1951–59, 2006.

[52] Cfr., 15 U.S.C.§1681.

[53] Cfr., 45 C.F.R.164.512(f)(1)(ii); 45 C.F.R.164.512(f)(2).

[54] Cfr., 42 U.S.C.§§ 2000ff to 2000ff-11, 2012.

[55] Cfr., 15 U.S.C.§§ 6501–06.

[56] Cfr., 20 U.S.C.§ 1232, 2012.

[57] Cfr., 18 U.S.C.§ 1039; but see 18 U.S.C.§§ 2703(c)(1)(B), 2703(d).

[58] Cfr., 18 U.S.C.§ 2710, 1994.

[59]Cfr., RAJAGOPALAN Megha, *Cellphone Companies Will Share Your Location Data—Just Not with You*, in *PROPUBLICA*, 2012, *www.propublica.org*.

[60]Cfr., SULLIVAN Bob, *Who's Buying Cell Phone Records Online? Cops*, in *MSNBC*, 2006, *www.msnbc.msn.com*; BLOCK Robert, *Requests for Corporate Data Multiply: Businesses Juggle Law-Enforcement Demands for Information about Customers, Suppliers*, in *WALL ST. J.*, 2006, A4.

riconfezionati, in questo modo, tuttavia, il punto di raccolta originale viene oscurato diventando quasi sconosciuto[61]. La polizia, quindi, ha sempre di più il potere di conoscere informazioni personali sui sospettati e le aziende private, a loro volta, hanno sempre più difficoltà a proteggere i dati da richieste governative legittime, rischiando, così, ancora una volta, di sacrificare la protezione della privacy.

Per questi motivi il tema dei *big data* resta attualmente molto problematico.

1.2 Gli strumenti utilizzati per monitorare i big data

Tutte le attività che quotidianamente sono svolte sui dispositivi digitali producono dati. Si tratta di una grandissima quantità di informazioni, ottenute da molteplici fonti, che possono essere raccolte, analizzate e quindi anche valorizzate per poter aiutare a prendere decisioni migliori o economicamente più vantaggiose.

Ciò significa cambiare il modello di *data analysis* optando per approcci cosiddetti 'descrittivi', 'predittivi', 'prescrittivi', ossia sfruttando applicazioni di *big data analytics* attraverso le quali generare ''*insights*'' (intuizioni), conoscenze utili ai processi decisionali (anticipando per esempio i bisogni del cliente conoscendone in *real-time* preferenze ed abitudini) e informazioni necessarie e ''non scontate'' (ossia di non facile identificazione). Questi strumenti matematici consentono agli analisti di dati di indovinare collegamenti ed intuizioni, di difficile rilevazione, da una ingentissima quantità di informazioni[62].

Come esempio di una di queste intuizioni, il gigante della vendita al dettaglio *Target* ha trovato un modo per prevedere quando le donne sono incinte[63]. Studiando le donne che si sono iscritte a un registro dei bambini in negozio, Target ha notato che queste donne incinte auto-identificate

[61]Cfr., RAJAGOPALAN Megha, *Cellphone Companies Will Share Your Location Data—Just Not with You*, in *PROPUBLICA*, 2012, *www.propublica.org*.

[62]Cfr., LERMAN Jonas, *Big Data and Its Exclusions*, in *STAN* , 2013, ONLINE S, 57, 66; Exec. *Office of the President, Big data: seizing opportunities, preserving values* , 2014, 2.

[63]Cfr., DUHIGG Charles, *How Companies Learn Your Secrets*, in *N. Y. TIMES MAG.*, 2012.

condividevano un modello di acquisto simile e ripetuto. Costoro acquisterebbero integratori di acido folico e vitamine nel primo trimestre (per migliorare la salute prenatale), lozione non profumata nel secondo trimestre (a causa dell'accresciuta sensibilità olfattiva) e disinfettante per le mani nel periodo vicino alle data del parto (per proteggere il neonato dai germi). Quindi ora se gli acquisti di una donna seguono questo schema (anche se non si è iscritta a un registro dei bambini), Target la segnala come incinta[64].Questo significa, che con l'ausilio dei *big data*, possono emergere correlazione di acquisti di consumatori apparentemente non correlati; ciò conduce a previsioni future molto attendibili.

La polizia dei *big data*, come meglio diremo nel corso del capitolo successivo, si avvale di meccanismi simili: invece, della sorveglianza sui consumatori, l'obiettivo del*''big data policing''* è la sorveglianza criminale[65].

Le forze dell'ordine, infatti, possono, ad esempio, identificare gli spacciatori di droga da modelli di forniture (acquisto di minuscole borse a chiusura lampo, elastici, bilance digitali), transazioni sospette (deposito di contanti, acquisti *all-cash* di fascia alta) e modelli di viaggio (da e da una città di origine per la droga). Le informazioni acquisite, aiutano, in modo proattivo, la polizia a trovare indizi nascosti volti a identificare un possibile futuro criminale.

Cathy O'Neil ha scritto, nel suo libro, *Weapons of Math Destruction*, proprio come Amazon utilizza i dati per identificare l'acquirente c.d. "recidivo" (inteso come colui che acquista spesso lo stesso prodotto o prodotti similari), la polizia può utilizzare sistemi simili di analisi dati per prevedere un futuro criminale[66].

2. La classificazione dei *big data*

[64]*Ibidem.*

[65]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York, 2017, 19.

[66]Cfr., O'NEIL Cathy, *Weapons of math destruction: how big data in-creases inequality and threatens democracy*, 2016, 98.

I big data possono essere suddivisi in tre categorie: i *black data*, i *blue data*, i *bright data*, tutti questi dati mirano all'identificazione del rischio di criminalità.

2.1 I Black data

Con l'uso dei *big data* a fini di indagini da parte della polizia che ricorre a sistemi predittivi sorge un problema: quello dei ‘*'black data''*, ovverosia dati che spesso non sono suscettibili di elaborazione informatica.

Il concetto di *''black data''* presuppone tre problematiche che riguardano discriminazioni razziali, trasparenza, e questioni di diritto[67].

In primis i dati raccolti dalla polizia americana risultano spesso essere: pieni di pregiudizi espliciti ed impliciti legati a discorsi razziali; ''opachi'', in quanto elaborati da algoritmi matematicamente complessi e di difficile comprensione; e infine restano ancora aperte le questioni in ambito di *privacy* e delle relative disposizioni legislative carenti.

L'analisi predittiva utilizza gli algoritmi per sviluppare e identificare ''modelli di rischio'' basati sull'acquisizione di dati forniti dalla polizia[68]. Un esempio è quello della c.d. *''Heat list''*[69], una lista composta da individui che per l'area geografica in cui vivono, per le compagnie che frequentano, per ambiente famigliare o per il loro passato, rischiano maggiormente di delinquere.

Attualmente esistono tre grandi categorie di tecnologie[70] usate dalla polizia per l'acquisizione di dati: tecnologie predittive, tecnologie di sorveglianza e tecnologie di *data mining*[71], tutte queste tecnologie condividono il problema dei *''black data''*.

---

[67]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement,* New York, 2017, 131.

[68]Cfr., FERGUSON Andrew Guthrie, *Illuminating Black Data Policing*, in 15 Ohio St. J. Crim. L. 2018, 505, 503.

[69]*Ibidem.*

[70]*Ibidem.*

[71]Cfr., CRAWFORD Kate & SCHULTZ Jason, Big Data and Due Process: *Toward a Framework to Redress Predictive Privacy Harms,* in *B.C.*, 2014, 93, 104-05, 55 (predictive analytics); LEVINSON Rachel -*Waldman, Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, in *EMORY*, 2017, 527-534, 66 (surveillance); SEYBOLD Steven D., Note, *Somebody's Watching Me: Civilian Oversight of Data-CollectionTechnologies*, in *TEX.*,

Tramite utilizzo di queste tecnologie, infatti, se da una parte c'è stata una svolta nel procedimento investigativo, dall'altro si palesano problematiche lesive per la tutela degli individui.

Primo fra tutti rientra il problema della discriminazione razziale. Negli Stati Uniti, dove la polizia usufruisce regolarmente di queste tecnologie per l'acquisizione dei dati, si tende ad associare la criminalità al colore della pelle, in altre parole le aree geografiche, in cui risiedono particolari comunità di colore, diventano indice di criminalità. Nella prassi questo fenomeno ha portato ad un eccessivo controllo da parte della polizia di tali aree e di tali soggetti, presupponendo una loro propensione a delinquere, spesso non corrispondente alla realtà.

A complicare l'impatto razziale è il fatto che la criminalità tende a essere correlata alla povertà e in molte aree urbane anche quelle aree povere sono correlate alle comunità di colore[72].

A causa di questo fenomeno discriminatorio gli errori sulla valutazione della pericolosità di taluni soggetti proliferano; ciò si traduce nella valutazione di dati che influiscono sui punteggi di rischio della già citata *''Heat list''* e quindi sull'attenzione della polizia a tali individui non più basata su effettivi tassi di criminalità bensì su indici discriminatori.

I *''black data''* devono essere ''illuminati'' per poter essere utilizzati, occorre cioè estrapolare gli elementi derivanti dalle intuizioni algoritmiche senza che questi abbiano un impatto negativo sulla privacy e sulla libertà dei cittadini e senza che siano lesivi dei loro diritti[73].

La polizia dei *big data* soffre altresì di un problema di trasparenza[74]. La problematica nasce dal fatto che gli algoritmi di apprendimento agiscono autonomamente, analizzando una ingente quantità di dati e creando connessioni tra essi in assenza input o controllo umano, la polizia finisce così

2015, 1029-1032, 93(surveillance); ZARSKY Tal Z., *Governmental Data Mining and Its Alternatives*, in *PENN ST.*, 2011, 285-287, 116(data mining).

[72]Cfr., SMITH Jack IV, *'Minority Report' is Real-And It's Really Reporting Minorities*, *MIC*, 2015.

[73]Cfr., FERGUSON Andrew Guthrie, *Illuminating Black Data Policing*, in 15 Ohio St. J. Crim. L. 2018, 504, 503.

[74]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 136.

per affidarsi ad un elaborato fornito esclusivamente dalla macchina[75]. I dati diventano ‘’opachi’’, viene meno la chiarezza, occorre, così, affinché la polizia dei *big data* abbia successo, superare tre problemi di trasparenza che coinvolgono: barriere tecniche, barriere tecnologiche e barriere tattiche[76].

Partendo dalla prima questione l'uso di strumenti altamente tecnici lede la trasparenza[77], questo accade *in primis* perché la polizia che utilizza i *big data* non possiede le medesime competenze informatiche delle aziende private che analizzano i dati tramite algoritmi, restandone così sempre dipendente anche solo per assistenza tecnica. La polizia finisce per affidarsi completamente all'algoritmo senza essere in grado di articolare analisi sul suo funzionamento, per cui l'elaborato della macchina sfugge completamente a qualsiasi forma di controllo[78]. In altre parole, l'algoritmo analizza gli individui e calcola il cd "punteggio di rischio", ma l'agente di polizia non è in grado di spiegare le modalità con le quali è stato calcolato il punteggio, finendo per dipendere dalle società private che si occupano di analisi di dati e per affidarsi completamente all'algoritmo senza comprenderne il funzionamento[79].

Passando al tema problematico delle barriere tecnologiche è possibile affermare che la tecnologia, per sua natura, ostacola la trasparenza[80]. Il codice informatico e gli algoritmi, infatti, tendono a nascondere i meccanismi alla base del loro funzionamento di sistema[81] e le aziende che si occupano di dati, a loro volta, nascondono i sistemi di funzionamento, per proteggere il valore della loro tecnologia a livello commerciale[82]. La trasparenza rischia di essere lesa sempre di più in un futuro in cui si mira ad un apprendimento automatico da parte degli algoritmi indipendenti dall'*input* del programmatore della

[75]Cfr., KROLL Joshua A. et al., *Accountable Algorithms*, in *U. PA.*, 2017, 633-679-80, 165.

[76]Cfr., FERGUSON Andrew Guthrie, *Illuminating Black Data Policing*, in 15 Ohio St. J. Crim. L. 2018, 510, 503.

[77]*Ibidem.*

[78]*Ibidem.*

[79]*Ibidem.*

[80]Cfr., FERGUSON Andrew Guthrie, *Illuminating Black Data Policing*, in 15 Ohio St. J. Crim. L. 2018, 511, 503.

[81]Cfr., FORD Paul, *What is Code?*,in *BLOOMBERG BUSINESS WEEK*, 2015.

[82]Cfr., FERGUSON Andrew Guthrie, *Illuminating Black Data Policing*, in 15 Ohio St. J. Crim. L. 2018, 511, 503.

macchina. L'*output* finale finirebbe così per sfuggire completamente a qualsiasi forma di controllo del creatore, incapace di definire le forme di apprendimento e di analisi autonomi della macchina.

Ad aggravare le difficoltà tecniche e tecnologiche sono le c.d. tattiche della polizia[83]. Questa evita volontariamente la trasparenza per mantenere il proprio vantaggio tattico[84], ad esempio, nascondendo informazioni relative al posizionamento dei sensori di sorveglianza, o sul modo in cui viene creata la cd ''*Heat list''*, poiché rivelarle significherebbe perdere il vantaggio tattico investigativo sui sospettati[85]. Tale cautela deriva, quindi, dall'esigenza di garantire l'efficacia e la sicurezza delle indagini[86].

Le conseguenze di questi problemi di trasparenza creano un vero e proprio ostacolo all'uso efficace delle tecnologie di polizia dei *big data*[87].

La complessità di questi meccanismi conduce alla necessità di ricorrere a terzi per l'interpretazione dei dati, esternalizzando conoscenze riservate della polizia. Sia per la polizia che per le comunità, le barriere tecniche, tecnologiche e tattiche rendono difficile comprendere se i sistemi di apprendimento automatizzato siano davvero efficaci[88].

L'incapacità di affrontare questi problemi di trasparenza rischia di delegittimare le strategie basate sui *big data*, anche se le tecnologie aiutano spesso la polizia.

La spinta alla trasparenza ha condotto a qualche cambiamento; ad esempio, nuove società di polizia predittiva, in un'ottica di maggiore chiarezza, hanno pubblicato il loro codice informatico di base e descritto i loro modelli informatici per rimuovere i pregiudizi, altre hanno tentato di spiegare il

---

[83]Cfr., FERGUSON Andrew Guthrie, *Illuminating Black Data Policing*, in 15 Ohio St. J. Crim. L. 2018, 512, 503.

[84]*Ibidem.*

[85]Cfr., HUROWITZ Noah, *NYPD Terrorism Boss Blasts Council Surveillance Oversight Bill as 'Insane,' DNAINFO*, 2017**,** (quoting MILLER John, *Deputy Commissioner of Intelligence and Counterterrorism*, "Terrorists and criminals do their due diligence and they literally study and adapt to evolving security measures.").

[86]Cfr., HARMON Rachel, *Why Do We (Still) Lack Data on Policing?*, in *MARQ.*, 2013, 1119-1129, 96.

[87]Cfr., FERGUSON Andrew Guthrie, *Illuminating Black Data Policing*, in 15 Ohio St. J. Crim. L. 2018, 513, 503.

[88]*Ibidem.*

funzionamento degli algoritmi predittivi[89].La questione della trasparenza resta aperta ma iniziano ad intravedersi spiragli di luce per tentare di risolverla.

Nell'uso dei *big data* il problema di fondo resta quello della loro affidabilità; in altre parole, occorre che la polizia ne faccia uso senza tradurre il sospetto in un vero e proprio indice di pericolosità.

L'approccio dell'azienda informatica di analisi dati *HunchLab*, per mitigare il problema, è quello di fornire meno informazioni agli agenti di polizia: '' Non diciamo loro la probabilità che si verifichi una rapina, perché le persone si attaccano alle probabilità''[90]. Un tale cambiamento potrebbe evitare le preoccupazioni di un algoritmo che distorce il ragionevole sospetto, tuttavia, al momento, il dibattito sull'adeguato equilibrio tra efficacia delle informazioni e prevenzione dei pregiudizi non è stato risolto[91].

Per concludere il problema dei *''black data''* può essere superato[92], ma per farlo è necessario privare i dati dai pregiudizi che ne derivano ed esplicare il funzionamento degli algoritmi predittivi in un'ottica di maggiore trasparenza, tutelando i diritti degli individui. Nel futuro delle indagini occorrerebbe, quindi, che la polizia incrementasse le proprie conoscenze tecnologiche in modo da essere in grado di conoscere i processi algoritmici alla base dei *big data*.

2.2 I *Blue data*

I c.d. *''blue data''* rispecchiano le tecnologie di sorveglianza sviluppate per la polizia, tra cui: mappatura del crimine, *''heat lists''*, monitoraggio in tempo reale (*real time monitoring*), *data mining*, sospetto probabilistico e

[89]Cfr., KENNEDY Leslie et al., R*utgers ctr. on pub. sec., a multi-jurisdictional test of risk terrain modeling and a place-based evaluation of environmental risk-based patrol deployment strategies*, 2015.

[90]Cfr., FERGUSON Andrew Guthrie, *Illuminating Black Data Policing*, in 15 Ohio St. J. Crim. L. 2018, 523, 503.

[91]*Ibidem.*

[92]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 142.

targeting predittivo[93].In altre parole, si parla di *big data* che svolgono un ruolo nel miglioramento dell'efficacia dell'azione della polizia, prevenendo un eccessivo uso della forza.

Per mappatura del crimine si intende un sistema di controllo della polizia basato su dati di geo-localizzazione[94]. La polizia, infatti, associa spesso modelli di criminalità ad alcuni quartieri con individui a maggior ''rischio'' di delinquere. Sussiste un problema di fondo, tramite questi modelli di localizzazione è possibile stabilire dove è avvenuto un crimine, ma non la posizione della polizia in quel preciso momento. Per colmare questa lacuna, attualmente, negli Stati Uniti, è possibile conoscere le interazioni tra polizia e cittadini tramite apposite ''schede di contatto'' (*contact cards*)[95]. A New York, per esempio, la polizia compila il c.d. *''UF-250 card''*, una scheda che memorizza la posizione esatta di ogni interazione polizia-cittadino[96]. Questi dati di localizzazione vengono caricati in database che possono essere utilizzati per tracciare i principali luoghi di contatti polizia-cittadini[97].

La mappatura del crimine risulta quindi composta da una stima di luoghi considerati ''caldi'' ossia ad alto tasso statistico di criminalità, insieme alla localizzazione in tempo reale delle pattuglie di polizia e dell'interazione con i cittadini.

La nuova tecnologia GPS di tracciamento della polizia è, quindi, in tempo reale. Questo meccanismo di localizzazione potrebbe essere molto utile nel futuro, migliorando l'efficienza e l'efficacia dell'intervento delle forze di polizia[98] e potrebbe offrire un nuovo modo per misurare i tempi di risposta alle chiamate di emergenza[99]. Si pensi ad esempio ad una rapina e alla necessità di

---

[93]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 143.

[94]*Ibidem.*

[95]*Ibidem.*

[96]Cfr., HARCOURT Bernard E. & MEARES Tracey L., *Randomization and the Fourth Amendment*, in *U. CHI.* 2011, 809-862, 78, 210.

[97]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 146.

[98]*Ibidem.*

[99]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 146.

inviare rinforzi; tramite questi *database* sarebbe possibile rintracciare i poliziotti vicini e condurli, nel minor tempo possibile, presso il luogo del delitto tramite la tecnologia del monitoraggio in tempo reale del *locus commissi delicti* e degli agenti di polizia di pattuglia.

In generale gli algoritmi predittivi, che analizzano il comportamento degli individui, non prevedono chi commetterà un atto criminoso, ma analizzano i fattori di rischio che rendono tale comportamento più probabile[100].Questo stesso meccanismo può essere applicato anche agli agenti di polizia, identificando quelli più a ‘’rischio’’ di interazioni negative con i civili o dell'uso della forza[101].

Gli studi hanno dimostrato che molte denunce, legate all'uso sproporzionato della forza, sono indirizzate solo ad un piccolo numero di ufficiali[102].Ci si chiede se, tramite i c.d. *‘’risk flags’’*, le c.d. bandiere di rischio, sia possibile riconoscere gli agenti, potenzialmente propensi all'uso sproporzionato della coattività, prima che utilizzino in modo inappropriato la forza.

Rayid Ghani, il direttore del Center for Data Science and Public Policy dell'Università di Chicago, ha iniziato a lavorare su una soluzione al problema, collaborando con il dipartimento di polizia di Charlotte-Mecklenburg, e basandosi su dati accumulati in quindici anni sul personale[103], su arresti, azioni di polizia[104]e molto altro. Il gruppo di ricerca ha, così, sviluppato un algoritmo predittivo con il compito di sviluppare una stima delle interazioni negative polizia-cittadino[105]. Come ha spiegato Ghani: ‘’L'idea è quella di prendere dati da questi dipartimenti di polizia e aiutarli a predire quali agenti sono a rischio

[100]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 147.

[101]*Ibidem.*

[102]Cfr., KRAJICEK David J., *What's the Best Way to Weed Out Potential Killer Cops*?, in *AITER-NET*, 2016.

[103]Cfr., LEE Jeaeh, *Can Data Predict Which Cops Are Most Likely to Misbehave in the Future?* , in *MOTHER JONES*, 2016.

[104]Cfr., GORDON Michad, *CMPD's Goal: To Predict Misconduct before It Can Happen*, in *CHARLOTTE OBSERVER*, 2016.

[105]Cfr., LEE Jeaeh, *Can Data Predict Which Cops Are Most Likely to Misbehave in the Future?* , in *MOTHER JONES*, 2016.

di comportamenti inappropriati… E se è possibile rilevarli presto, possono esserci interventi volti alla loro corretta formazione e consulenza[106]''.

Tramite questo sistema è possibile valutare l'evoluzione dei nuovi sistemi di formazione ''personalizzati'' basati sul ''rischio'', enfatizzando la riabilitazione piuttosto che la punizione[107]. Il sistema predittivo di Ghani ha offerto un approccio più mirato sui poliziotti, valutando anche le variabili che spesso conducevano ad un eccessivo uso della forza come lo stress[108]. Ad esempio, alcune intuizioni algoritmiche hanno riscontrato, nei casi di violenza domestica, un uso sproporzionato delle armi da parte della polizia, a causa della cattiva gestione emotiva e dello stress. Ci si è resi conto, però, che inviando tre o quattro agenti a controllare la scena del crimine anziché uno o due, le probabilità di violenza sono diminuite drasticamente, questo a causa di un maggior controllo della situazione[109].

La prossima fase nella raccolta dei *''blue data''* consiste nell'analisi dei metodi di estrazione di dati di polizia volti a migliorare l'efficienza, l'efficacia, l'accuratezza delle attività, senza che questa sia pregiudizievole, senza che si incorra in errori, o problemi di trasparenza[110].

Un gruppo multidisciplinare di studiosi – David Sklansky, Sharad Goel, Ravi Shroff e Maya Perlman, rispettivamente un professore di legge, un professore di ingegneria, uno scienziato di dati, e uno studente di legge – ha dimostrato che i big data possono migliorare l'accuratezza predittiva delle perquisizioni[111].

L'analisi è stata fatta su casi di polizia di New York tra gli anni 2008-2010; i ricercatori hanno creato il c.d. *''Stop-level hit rate'' (SHR)*[112], un sistema in

---

[106]Cfr., GHANI Rayid, intervista di CORNISH Audie, *Can Big Data Help Head Off Police Misconduct?, ALL TECH CONSIDERED* in *NPR radio broadcast,* 2016.

[107]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 148.

[108]*Ibidem.*

[109]Cfr., GHANI Rayid, intervista di CORNISH Audie, *Can Big Data Help Head Off Police Misconduct?, ALL TECH CONSIDERED* in *NPR radio broadcast,* 2016.

[110]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 150.

[111]Cfr., GOEL Sharad et al., *Combatting Police Discrimination in the Age of Big Data*, in *NEW. CRIM.*, 2017, 6.

[112]*Ibidem.*

grado di calcolare il tasso di probabilità, prima di una perquisizione, del possesso di un'arma da parte di un individuo[113].L'indagine è stata effettuata confrontando un ingente numero di'*''UF-250 cards''*, quindi i dati riconducibili alla posizione GPS dei poliziotti, come data, ora, luogo di fermo, con alcuni fattori di sospetto per la perquisizione come movimenti furtivi o aree ad alta criminalità, rivelando una percentuale di sospetti effettivamente utili al ritrovamento dell'arma e una percentuale di sospetti fuorvianti[114].Alla fine della ricerca, il modello includeva più di settemila caratteristiche predittive volte a comprendere i fattori-chiave per il recupero con successo di un'arma[115].

Gli studiosi hanno poi applicato il modello predittivo negli anni seguenti, rispettivamente dal 2011 al 2012 per monitorare l'efficacia delle previsioni, scoprendo che il tasso di successo per ritrovamento di un'arma era dell'83%[116]. Usando il metodo SHR, tramite l'analisi dei dati della polizia, è possibile, quindi, comprendere quali sospetti sono effettivamente correlati a comportamenti criminali e quali no[117], perfezionando l'idea di autentico ''rischio'' e indirizzando le strategie investigative in tal senso.

In definitiva, i *''blue data''* aiutano a scoprire nuove tecniche efficaci per la polizia e riducono altresì i vecchi pregiudizi[118] che associavano le aree di rischio a motivi razziali, ricollegando esclusivamente i sospetti fondati e comprovati all'effettivo rischio criminoso.

Le intuizioni basate sui dati in merito all'accuratezza delle azioni di polizia e ai pregiudizi razziali compaiono in uno studio del 2016 – *Data for Change*– dell'Università di Standford[119]. Il gruppo di ricerca, guidato da Jennifer

---

[113]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 150.

[114]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 151.

[115]Cfr., GOEL Sharad et al., *Combatting Police Discrimination in the Age of Big Data*, in *NEW. CRIM.*, 2017, 27.

[116]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 151.

[117]*Ibidem.*

[118]*Ibidem.*

[119]Cfr., HETEY Rebecca C. et al, *Data, for Change: A Statistical Analysis of Police Stops, Searches, Handcuffings, and Arrests in Oakland, Calif*, in *STANFORD SPARQ* 2013-2014; ID., *SOCIAL PSYCHOLOGICAL ANSWERS TO REAL- WORLD QUESTIONS* , 2016.

Eberhardt[120], ha collaborato con il dipartimento di polizia di Oakland per studiarne i dati. Tramite il processo di *''data-mining''* gli studiosi hanno analizzato, tramite strumenti informatici, i c.d. *''stop data''*, dati relativi a fermi della polizia rivolti a pedoni e conducenti di automobili. Successivamente hanno confrontato, tramite monitoraggio audiovisivo, il linguaggio rivolto dai poliziotti verso i civili e da ultimo le relazioni della polizia relative ai fermi[121]. L'obiettivo consisteva nella valutazione del comportamento degli agenti verso i cittadini[122].

Dopo aver analizzato più di trentamila dati i ricercatori sono giunti alla conclusione che la polizia del dipartimento di Oakland risultava essere tendenzialmente discriminatoria, considerando che il 60% dei soggetti sottoposti al controllo della polizia era composto da cittadini afroamericani, rappresentanti circa il 28% della popolazione locale[123]. Questo dato risulta essere pregiudizievole in quanto la percentuale di rischio, nella maggior parte dei casi, non coincideva con la pericolosità effettiva dei cittadini arrestati.

Nel ''Data for Change'' e nella relazione di accompagnamento ''Strategies for Change'', i ricercatori di Standford forniscono, quindi, nuovi metodi per studiare il comportamento della polizia nelle interazioni con i cittadini[124]. Lo studio di Standford ha rivelato che: ''Gli uomini afroamericani, sono stati ammanettati, rispetto a quando sono stati sottoposti a controlli, una volta su quattro, gli uomini bianchi, invece, soltanto una volta su quindici.

Anche dopo aver controllato i tassi di criminalità del quartiere, i dati demografici e molti altri fattori, le analisi hanno dimostrato che gli agenti (*Oakland Police Department*) hanno ammanettato significativamente più

---

[120]*Ibidem.*

[121]*Ibidem.*

[122]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 151.

[123]Cfr., HETEY Rebecca C. et al, *Data, for Change: A Statistical Analysis of Police Stops, Searches, Handcuffings, and Arrests in Oakland, Calif*, in *STANFORD SPARQ* 2013-2014; ID., *Social psychological answers to real- world questions,* 2016.

[124]Cfr., EBERHARDT Jennifer, *Strategies for Change: Research Initiatives and Recommendations to Improve Police-Community Relations in Oakland, Calif*; ID., *Social psychological answers to real-world questions* in *STANFORD SPARQ*, 2016, 12.

afroamericani che bianchi[125]''. I ricercatori, mediante lo studio dei dati della polizia, hanno scoperto ulteriormente che il linguaggio utilizzato dai singoli poliziotti variava a seconda della razza del cittadino, divenendo meno rispettoso nei confronti degli afroamericani[126].

Nel futuro la capacità degli algoritmi, di monitorare le attività in tempo reale, consentirebbe agli ufficiali di polizia di monitorare l'attività dei singoli agenti e migliorarne l'efficacia, valutandone la formazione[127]. Tale sistema avrebbe bisogno di una sorveglianza continua, ma aiuterebbe a risolvere i problemi destabilizzanti della polizia degli Stati Uniti come il pregiudizio razziale e l'uso sproporzionato della forza[128].

Dall'indagine sui *''blue data''* si riscontra, mappando, tracciando[129] le attività e gli spostamenti degli agenti di polizia, che i pregiudizi razziali e l'uso illegittimo della forza non derivano da pochi, singoli poliziotti, ma costituiscono un problema sistematico-culturale. Con l'ausilio dei *''blue data''*, quindi, è possibile studiare le debolezze del sistema nella sua interezza[130], offrendo la possibilità di prevenire i rischi di comportamenti degli agenti incoerenti con la buona condotta delle loro mansioni.

Il Dipartimento di Giustizia degli Stati Uniti ha supervisionato e indagato, già nel passato, su dozzine di dipartimenti di polizia per accertare la lesione di diritti civili[131]; la tecnologia dei *big data* potrebbe dare un grande supporto nel futuro prossimo. Il governo federale, attraverso il *Department of Justice Office of Community Oriented Policing Services (COPS)*, ha infatti accettato di finanziare la formazione e l'assistenza tecnica per i dipartimenti di polizia

---

[125]*Ivi,* 14.

[126]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 155.

[127]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 157.

[128]*Ibidem.*

[129]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 162.

[130]*Ibidem.*

[131]Cfr., SIMMONS Kami Chavis, ''*The Politics of Policing: Ensuring Stakeholder Collaboration in the Federal Reform of Local Law Enforcement Agencies*'', in *J. CRIM. L. & CRIMINOL.*, 2008, 489-490, 98; WALKER Samuel, *The New Paradigm of Police Ac-countability: The U.S. Justice Department "Pattern or Practice" Suits in Context*, in *ST. LOUIS U. PUB.*, 2003, 3-8, 22.

locale che hanno interesse ad impegnarsi nella *''Police Data Initiative''*[132]. Inoltre, alcune aziende private e organizzazioni *non profit* come la *''Police Foundation''*, *''*l'*International Association of Chiefs of Police''*, *la ''Sunlight Foundation''* e altre hanno accettato di fornire ulteriori strumenti tecnici e digitali per consentire a più persone di accedere e utilizzare i dati[133].L'uso dei *''blue data''* può così portare a risolvere, nel futuro, ogni pregiudizio sistemico e aprire la strada ad un'ottica di trasparenza dell'azione di polizia basata su strumenti tecnologici avanzati.

2.3 I Bright data

Le tecnologie di polizia dei *big data* hanno tutte un elemento comune: l'identificazione dei fattori di rischio predittivi legati all'attività criminale[134]. Per *''bright data''* si intendono quei dati che rivelano problemi e modelli nascosti, quindi le correlazioni tra i ''rischi'' e i relativi possibili rimedi.

Un esempio è quello dei ''*PredPol*'' e ''*HunchLab*''[135], due *software* in grado di determinare luoghi di alto rischio di criminalità e quindi aiutare la polizia alla prevenzione del crimine in tali aree. Per essere più concreti, questi algoritmi predittivi sono in grado di identificare, secondo stime probabilistiche, il rischio di furto di auto in un determinato luogo e in quali circostanze, consentendo alla polizia di inviare pattuglie in via precauzionale.

Il *software* RTM[136] (*Risk Terrain Modelling*) ha proposto invece, per ridurre i fattori di rischio e rendere taluni luoghi meno attraenti per l'azione criminale, l'applicazione di più sanzioni stradali, sempre con l'ausilio di un maggiore controllo della polizia. Altre soluzioni potrebbero essere quelle di installare videosorveglianza in tempo reale nelle aree ad alto rischio.

---

[132]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 166.

[133]Cfr., White House, Office of the Press Secretary, *Fact sheet: white house police data initiative highlights new commitments*, 2016.

[134]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 167.

[135]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 168.

[136]*Ibidem.*

Tutti questi rimedi hanno un unico *vulnus*; necessitano sempre dell'azione della polizia. Tramite l'intuizione tecnologica derivante dai *''bright data''* c'è una svolta: ciò che diventa rilevante come rimedio è l'azione umana nel suo complesso. In altre parole, è possibile rimediare alla vulnerabilità ambientale che conduce all'alto rischio di furto di automobili tramite installazione di cancelli, serrature, pass di sicurezza nei parcheggi, sensibilizzazione educativa dei residenti dei quartieri a ''rischio''[137]. Tutte queste operazioni possono essere messe in atto anche dai comuni cittadini, diminuendo il controllo costante della polizia.

L'intervento delle forze di polizia può essere, infatti, uno degli elementi principali nel sistema per risolvere il crimine, ma non deve essere quello essenziale per ridurne il rischio[138].Ricorrere sempre al rimedio del richiamo delle forze dell'ordine condurrebbe ad una risoluzione del problema della delinquenza soltanto temporanea, con la conseguente probabilità di non eliminare totalmente le vulnerabilità ambientali dei luoghi c.d. ''caldi'' (ad alto tasso di criminalità) e di quelli più poveri. D'altro canto, sensibilizzando la comunità sul tema mediante maggiori sanzioni sul traffico, più controlli su aree abbandonate appetibili per il crimine, con un sistema di *''zoning enforcement''*[139], potrebbero esserci impatti favorevoli sulla delittuosità a lungo termine, prevenendola con maggior successo.

I modelli dei *big data* possono aiutare a visualizzare i fattori di rischio della criminalità anche in base all'età e a contesto sociale; un esempio utile è rappresentato dalla già citata mappatura del crimine[140] un sistema che non ha fermato il crimine o lo ha risolto, ma ha permesso un'attenzione più focalizzata alle particolari aree di rischio di maggiore delinquenza[141].Si pensi ora ad un medesimo sistema ma in grado di visualizzare i bisogni sociali: la c.d. ''mappa

[137]*Ibidem.*

[138]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 169.

[139]*Ibidem.*

[140]V. paragrafo ''blue data'', 16.

[141]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 170.

del rischio'' (''*risk map*'')[142]. È possibile immaginare un servizio simile all'algoritmo di *Beware*[143], società che cataloga i dati dei consumatori, e applicarlo nella realtà per identificare i soggetti bisognosi, anziché i soggetti potenzialmente pericolosi.

Dall'analisi è efficacemente riscontrabile se i servizi sociali competenti siano o meno sono vicini alle persone bisognose e incrementare che le poche risorse disponibili per la necessità. La mappa potrebbe mostrare uno squilibrio con l'esigenza di più finanziamenti e più risorse. I modelli di problemi sociali potrebbero, così, essere visualizzati, in aggiunta al crimine, su mappe di rischio in tutta la città, per migliorare le condizioni globali[144].

L'idea di una mappa del rischio basata sui *bright data* è quella di rendere visibili gli specifici bisogni sociali, quindi, porre l'attenzione sulla relativa azione correttiva[145]. Applicando le modalità di analisi dati dei dirigenti della polizia per ridurre i numeri della criminalità, anche alle condizioni sociali i dirigenti della città potrebbero ridurre le situazioni di povertà in modo mirato.

Questa idea di trasformare la raccolta di dati, simile a CompStat (il *Computer Stastistics*), programma di informatizzazione utilizzato dai dipartimenti di polizia, in strategie di *bright data* per la responsabilità sociale e governativa è stata introdotta da Robert D. Behn, alla Kennedy *School of Government* di Harvard. Behn ha creato il concetto di "*PerformanceStat*" una strategia di leadership di *governance* basata sui dati[146].

Questo sistema consente di tracciare la percentuale di riduzione della criminalità e di reindirizzare la polizia nei principali luoghi a rischio di delinquenza, diminuendone la ricorrenza. Queste mappe dei rischi legate ai problemi sociali potrebbero anche aiutare gli agenti di polizia a svolgere il loro lavoro nel modo più efficiente possibile.

---

[142]*Ibidem.*

[143]*Ibidem.*

[144]*Ibidem.*

[145]*Ibidem.*

[146]Cfr., BEHN Robert D., *The PerformanceStat Potential: a Leadership Strategy for Producing Results*, 2014.

Ogni giorno la polizia affronta una serie di problemi sociali come povertà, gli incidenti legati alla salute mentale, ai reati giovanili. Mappare questi problemi sociali sarebbe molto utile per identificare i punti critici e catalogare le relative azioni di polizia, così come le relative lacune di servizio. Allo stesso modo in cui si possono vedere i punti ‘’caldi’’ della criminalità, si possono vedere i punti dolenti del bisogno sociale e fornire un adeguato intervento proattivo volto ad una maggiore consapevolezza dell'intervento delle forze dell'ordine.

Come esempio di mappatura di *bright data*, il *District of Columbia Fire and Emergency Medical Services Department* (Fireed EMS) e il *Department of BehavioralHealth* (DBH) interagiscono quotidianamente con una serie di dati relativi alla salute[147]. Dall'analisi si è riscontrato il problema dell'overdose; spesso, infatti il paziente veniva condotto in ospedale, anche dalla polizia, che chiudeva il caso subito dopo, trascurando eventuali ricadute del tossicodipendente assai frequenti nella realtà.

Nell'estate del 2015, D.C. Firee EMS, insieme al DBH, hanno deciso di cambiare la situazione mappando i dati sull'overdosedi droga[148].

Le due agenzie hanno fissato l'obiettivo di garantire ad ogni persona che ha assunto talmente tante sostanze al punto da finire in overdose, di ricevere una visita di controllo, entro sette giorni dall'evento dell'overdose, da un *team* di professionisti addestrato nella consulenza sull'abuso di sostanze. Il gruppo offrirebbe così un supporto al tossicodipendente come l'opportunità di condurlo in una struttura di recupero e trattamento (DBH)[149].

Naturalmente, la mappatura della salute pubblica ad ausilio delle forze dell'ordine può creare seri problemi di privacy. Per risolvere tale questione D.C. Fireed EMS, nel progetto pilota, non ha condiviso i nomi o gli indirizzi di casa delle vittime di overdose di droga con le forze dell'ordine e le informazioni

[147]Cfr., SA'ADAH Rafael, *Assistant Chief, District of Columbia Fire and Emergency Medical Services Department*, 2016.

[148]Cfr., BRESS Jessica, *Policy Advosor at DC Department of Behavioral Health, Presentation, Final Analysis del SBIRT Pilot Program 30/05/2015—02/08/2015;* SA'ADAH Rafael, *Acting Deputy Fire Chief, District of Columbia Fire and Emergency Medical Services Department,* 2015.

[149]*Ibidem.*

sulla posizione e sui tipi di overdose sono state de-identificate e aggregate in blocchi di unità o sottounità geografiche simili prima di essere mappate e condivise con le forze dell'ordine[150]. Nonostante questi accorgimenti, restano tematiche problematiche sulla privacy in tema di geo-posizione dei tossicodipendenti.

3. I Metadati

I *big data* possono essere rivelatori di indici criminali anche tracciando le comunicazioni. L'acquisizione dell'ingentissimo numero di informazioni telefoniche (*phone records*) può essere meravigliosamente utile per le indagini, in forza della potenza dei metadati di collegare le interazioni tra i vari numeri di cellulare, mostrando connessioni altrimenti invisibili[151]. Sono strumenti utili soprattutto per quanto riguarda la geo-localizzazione del cellulare e quindi peril controllo degli spostamenti di alcuni soggetti ritenuti ''rischiosi''.

I c.d. metadati sono i "dati sui dati", informazioni che, applicate al contesto telefonico si traducono nel numero, nei contatti, nell'ora, la data e il luogo della chiamata, ma non del suo contenuto[152]. I metadati sono una creazione derivante dai *big data*, utile perché i computer potenti possono tracciare e confrontare itre miliardi di telefonate fatte negli Stati Uniti e nel mondo ogni giorno[153]. I metadati derivano anche dall'uso di Internet e del computer, dai *post* sui *social media*, dalle fotografie digitali e praticamente da ogni attività digitale svolta al giorno d'oggi[154]. In altre parole, tracciando il numero telefonico di un particolare sospettato è possibile accedere a tutti i soggetti che vi hanno interagito comunicando con il cellulare.

---

[150]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 172.

[151]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 111.

[152]Cfr., KIFT Paula H. e NISSENBAUM Helen, Metadata in Context: *An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program*, in *ISJLP*, 2017, 13.

[153]Cfr., Dichiarazione del Prof. FELTEN Edward, *Civil Liberties Union*, in *S.D.N.Y.*, 2013, 13-cv-03993, 14.

[154]Cfr., POMERANTZ Jeffrey, *METADATA, The MIT Press*, Massachusetts, 2015, 3 e 13.

La questione in merito ai metadati telefonici ha avuto inizio con la sconcertante rivelazione di Edward Snowden, informatico e attivista statunitense, sul fatto che la *National Security Agency*(NSA) stava raccogliendo metadati di registrazione telefonica[155].Attraverso il programma di metadati di telefonia dell'agenzia, la NSA ha raccolto dati di localizzazione sulle chiamate, l'identità, IMSI dei chiamanti e la durata delle chiamate ma non il loro contenuto[156].L'azione dell'NSA consisterebbe, quindi, nel suddividere e analizzare i dati in base ad informazioni su specifici e mirati numeri di telefono[157]. Non si tratta di intercettazioni perché non si mira a conoscere il contenuto della chiamata, bensì le informazioni relative al tracciamento.

Ma come funziona il sistema dei metadati? Le connessioni tra i numeri oggetto di controllo vengono collegate in "*hops*" (i c.d. salti), il che significa collegare tutti i numeri che hanno avuto contatti con il numero di telefono da monitorare[158]. Quindi, ad esempio, il numero di telefono di un bersaglio terrorista internazionale[159] potrebbe essere collegato a una, due o tre chiamate, fino a creare una rete di collegamenti tra tutte le chiamate in uscita e in entrata (uno, due, tre *hops*). La c.d. mappa della rete "*hops*" rivela, così, le possibili connessioni tra sospetti e minacce per l'*intelligence*.

Nel contenzioso sulla costituzionalità del programma NSA, Edward Felten, direttore del *Center for Information Technology Policy della Princeton University*, ha dettagliato la natura rivelatrice dei metadati[160]:«Anche se questi metadati potrebbero sembrare, a prima impressione, banalmente'' informazioni riguardanti chiamate a svariati numeri di cellulare'', l'analisi dei metadati della telefonia spesso rivela informazioni che tradizionalmente potevano essere ottenute solo esaminando il contenuto delle comunicazioni. Cioè, i metadati

[155]Cfr., KIFT Paula H. e NISSENBAUM Helen, Metadata in Context: *An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program*, in *ISJLP*, 2017, 13.

[156]Cfr., LITHWICK Dahlia e VLADECK Steve, *Taking the "Meh" out of Metadata*, in *SLATE*, 2013.

[157]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 111.

[158]*Ibidem.*

[159]*Ibidem.*

[160]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 112.

sono spesso dei *proxy*, sistemi che elaborano e gestiscono il grande traffico di informazioni, volti ad ottenere dati sul chiamante o sul chiamato, compresi, talvolta, i contenuti delle chiamate. Nell'esempio più semplice, alcuni numeri di telefono vengono utilizzati per un unico scopo, ossia quello di rivelare, tramite qualsiasi contatto telefonico, informazioni, spesso sensibili, sul chiamante. Gli esempi includono le *hotlines* di supporto (linee telefoniche di assistenza) per le vittime di violenza domestica e stupro, o addirittura un una linea diretta specifica di supporto delle forze armate per le vittime di stupro. Allo stesso modo, esistono numerose *hotlines* per le persone a rischio di suicidio, compresi servizi specifici per gli anziani e gli adolescenti, e i soggetti fragili in generale. Esistono anche *hotlines* per chi soffre di varie forme di dipendenza, come alcol, droga e gioco d'azzardo[161]».

I metadati risultano tanto utili quanto potenzialmente lesivi sul piano della *privacy* per cui emergono delle criticità. Per comprovare la potenza dell'analisi dei metadati si pensi all'esempio offerto da Felten per mostrarne il meccanismo applicativo: «Si consideri una giovane donna che chiama il suo ginecologo; poi chiama immediatamente sua madre; poi un uomo con cui, negli ultimi mesi, aveva ripetutamente parlato al telefono dopo le23:00; il tutto seguito da una chiamata a un centro di pianificazione familiare che illustra anche la possibilità di una interruzione volontaria di gravidanza. Dal quadro emerge una situazione complessiva che non sarebbe stata così evidente esaminando le informazioni di una singola telefonata[162]».

Le informazioni telefoniche diventano così rilevanti perché collegate con una chiamata e poi un'altra ancora e così via, ecco così dimostrata la forza invasiva dei metadati, capace di offrire un completo screening sulla vita e sulla personalità di uno o più individui. Immaginare un tale meccanismo applicato su larga scala mostra non poche difficoltà nell'ambito di tutela dei diritti, che rischiano di essere lesi da una tale pervasività.

[161]Cfr., Dichiarazione del Prof. FELTEN Edward, *Civil Liberties Union*, in *S.D.N.Y.*, 2013, 13-cv-03993, 14.

[162]*Ivi,* 17 s.

Uno studio della *Stanford University* ha confermato la potenza invasiva dei metadati[163]. Lo studio ha coinvolto 823 partecipanti volontari che hanno fornito l'accesso alle informazioni sui metadati su251.788 chiamate e 1.23439 messaggi[164].

L'analisi ha cercato di creare un *set* di dati che potesse testare il funzionamento del programma di ricerca dei metadati della NSA[165]. Lo studio ha fornito quattro principali modalità di estrazione di informazioni rilevanti per la polizia dei big data. *In primis* tramite i c.d. ''*hops*'' sono state create connessioni su tutti i duecentocinquantamila numeri di telefono. In secondo luogo, tramite il medesimo meccanismo, è stato possibile conoscere i nomi degli intestatari dei numeri di telefono anche se erano celati attraverso l'uso di ricerche sui *social media* e suI nternet. In questo modo anche i numeri ''deidentificati'' potevano essere ''ridentificati'', scoprendo, così, l'identità dei possessori dei numeri di cellulare. I ricercatori hanno concluso, quindi: "I numeri di telefono sono tutti tendenzialmente identificabili"[166]. In terzo luogo, studiando il contenuto delle chiamate, si potrebbero potenzialmente determinare informazioni sulla vita privata delle persone, compresi i dati sensibili, come ad esempio le condizioni mediche del chiamante[167].

I ricercatori potrebbero persino sviluppare sospetti su taluni soggetti per particolari crimini, e i contatti con possibili concorrenti nel reato[168].

Nonostante i problemi di privacy, il Governo degli Stati Uniti ha costantemente sostenuto il programma di metadati considerando il fatto che si trattava di un sistema di raccolta dati non basato sui contenuti, quanto più su connessioni e interazioni tra più informazioni telefoniche. Gli utenti, infatti, condividono già consapevolmente le informazioni relative ai dati associati al

---

[163]Cfr., MAYER Jonathan, MITCHELL John C., MUTCHLER Patrick, *Evaluating the Privacy Properties of Telephone Metadata*, in *PNAS*, 2016, 5536, 113.

[164]*Ibidem.*

[165]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 112.

[166]Cfr., MAYER Jonathan, MITCHELL John C., MUTCHLER Patrick, *Evaluating the Privacy Properties of Telephone Metadata*, in *PNAS*, 2016, 5540, 113.

[167]*Ibidem.*

[168]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 113.

numero di cellulare con il gestore telefonico. Inoltre, ha sostenuto che a causa delle restrizioni all'accesso e alla diffusione dei dati, il programma non risultava violare i diritti costituzionali dei cittadini degli Stati Uniti[169].

In secondo luogo, il Governo ha sostenuto che era ragionevole l'analisi dei dati, volta alla prevenzione della delinquenza, seppur in forma non eccessivamente pervasiva, confrontata al prevalente interesse di controllo e sicurezza nazionale[170].

La NSA ha raccolto molte informazioni mediante compagnie telefoniche come *AT&T*, società capaci di conservare i metadati telefonici per anni; si stimano infatti circa trilioni di dati e registrazioni telefoniche ricercabili nel software di *AT&T*[171]. Alcune forze dell'ordine come la DEA hanno avuto accesso a questo super database di metadati attraverso un super motore di ricerca, tutt'ora parzialmente segreto, chiamato '*'Hemisphere Project''*[172]. La *Drug Enforcement Agency* ha persino permesso ad *AT&T* di lavorare accanto agli agenti.

Un altro sistema utilizzato ad ausilio delle forze dell'ordine, è "*Google on Steroids*" che consente agli investigatori di cercare connessioni tra numeri e posizioni di qualsiasi chiamata che passa attraverso il database di *AT&T*[173]. Le forze di polizia possono avere accesso a tali informazioni, per la prevenzione del crimine, anche senza un mandato giudiziario[174].

---

[169]Cfr., KLAYMAN v. Obama (Klayman I), 957 F. Supp. 2d 1, 41 (D.D.C. 2013); *Am. Civil Liberties Union v. Clapper*, 959 F. Supp. 2d 724, 752, S.D.N.Y. 2013.; FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 113.

[170]Cfr., *Directives Pursuant to Section 1053 of Foreign Intelligence Surveillance Act*, in *Foreign Int. Surv.* , 2008, 3d, 1004-1006, 551; v. MARGULIES Peter, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection after Snowden*, in *HASTINGS* , 2014, 1, 51-57, 66 ; DONOHUE Laura K., *Bulk Metadata Collection: Statutory and Constitutional Considerations*, in *HARV.* e *PUB. POL' Y.*, 2014, 757-825, 37.

[171]Cfr., LIPP Kenneth, *AT&T Is Spying on Americans for Profit, New Documents Reveal*, in *DAILY BEAST*, 2016.

[172]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 114.

[173]Cfr., MAASS Dave e MACKEY Aaron, *Law Enforcement's Secret "Super Search Engine" Amasses Trillions of Phone Records for Decades*, in *ELECTRONIC FRONTIER FOUNDATION*, 2016.

[174]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 114.

Per bilanciare le esigenze di *privacy* e quelle di controllo governativo sulla criminalità, il Congresso ha vietato la raccolta indistinta di massa di metadati telefonici effettuata nel programma della NSA, permettendo però alle forze dell'ordine nazionali di ottenere l'accesso ai metadati per casi specifici di particolare rilevanza[175].

4. Il procedimento di acquisizione dei dati

Per *''data mining''* (estrazione di dati) si intende la ricerca, di grandi *set* di dati, volta a scoprire nuove intuizioni investigative[176]. Nelle azioni di polizia questo procedimento si traduce nell'utilizzare le informazioni, derivanti dall'analisi e dalla raccolta di ingenti quantità di dati, per scoprire e risolvere i crimini[177].

La polizia, infatti, negli Stati Uniti, utilizza regolarmente il procedimento di *''data mining''*quando deve acquisire informazioni su impronte digitali o confronto del DNA tramite informazioni raccolte in grandi database nazionali[178]. Questa operazione avviene tramite un *software* di *pattern-matching* (cioè di corrispondenza di modelli) che paragona le impronte digitali raccolte o i profili del DNA, con quelli presenti nel *database*, per trovare una corrispondenza[179]. L'FBI ha aumentato la sua capacità di ricerca costruendo un sofisticato *database* biometrico che include DNA, impronte digitali, impronte di palmi, impronte facciali, tatuaggi e scansioni dell'iride[180].

---

[175]Cfr., ACKERMAN Spencer, *FBI Quietly Changes Its Privacy Rules for Accessing NSA Data on Americans*, in *GUARDIAN*, 2016; COOKE Kristina e SHIFFMAN John, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, in *REUTERS*, 2013.

[176]Cfr., COLONNA Liane, *A Taxonomy and Classification of Data Mining*, in *SMU ScI.&TECH.*, 2013, 309-314 ,16.

[177]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 116.

[178]Cfr., MURPHY Erin, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, in *CAL.*, 2007, 721, 728-30, 95.

[179]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 116.

[180]Cfr., DONOHUE Laura K., *Technological Leap, Statutory Gap, and Constitutional Abyss:* SEP *Remote Biometric Identification Comes of Age*, in *MINN.* 2012, 407-413, 97.

Questo sistema di identificazione di nuova generazione, il *Next Generation Identification* (NGI), possiede la capacità di consentire, tramite la tecnologia del confronto dei *big data*, ad oltre diciottomila unità di forze dell'ordine, di ricercare informazioni nei database[181]. Allo stesso modo, l'FBI, con l'*U.S. Treasury* e la *Securities and Exchange Commission* (SEC) si affida ad algoritmi finanziari di *pattern-matching* per tenere traccia di depositi in contanti insoliti, trasferimenti internazionali o manipolazione delle azioni, utili per segnalare il rischio di reati quali il riciclaggio o l'evasione fiscale[182]. Tracciando il movimento del denaro attraverso i dati, potrebbero essere scoperte e perseguite, quindi, molte reti criminali.

Il *data mining* ha anche aiutato la polizia ad affrontare il problema della violenza domestica. A New York City, i dati hanno contribuito a identificare quegli individui con maggiori probabilità di esercitare violenza sui propri *partner*[183]. Per l'indagine gli agenti di polizia di New York, per un periodo di un anno, hanno risposto a 263.207 chiamate di emergenza per segnalazione di violenza domestica, e, vista la pericolosità del fenomeno e la sua possibile reiterazione, si sono avvalsi di un algoritmo capace di segnalare nelle chiamate parole come ''uccido'', ''alcol'', ''suicidio'', associandole agli indirizzi di provenienza delle telefonate[184]. Il risultato è stato quello di una migliore efficacia nell'azione di intervento grazie a programmi in grado di mappare le case, che si prevedeva fossero il luogo destinato alla futura violenza domestica, dare priorità alle chiamate provenienti da quella locazione ed effettuare controlli saltuari per scoraggiarne la ricommissione[185].

Anche i dati sugli acquisti dei consumatori possono essere ricercati per possibili indizi sull'attività illegale. Ad esempio, uno studio del Kentucky ha rilevato che le vendite di farmaci per il raffreddore con il principio attivo pseudoefedrina erano direttamente correlate ad un aumento della produzione

[181]Cfr., Comunicato stampa, FBI, *FBI Announces Full Operational Capability of the Next Generation Identification System*, 2014.

[182]Cfr., RICH Michael L., *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, in *U. PA.*, 2016, 871-876, 164.

[183]Cfr., GOLDSTEIN Joseph, *Police Take on Family Violence to Avert Death*, in *N. Y. TIMES*, 2013.

[184]*Ibidem.*

[185]*Ibidem.*

di metanfetamina e degli arresti di droga[186]. Come riportato dal Los Angeles Times, "In qualsiasi contea, un aumento delle vendite di pseudoefedrina di 13 grammi per 100 persone si è tradotto nella scoperta di un laboratorio di metanfetamina. I risultati suggeriscono che i database informatici potrebbero effettivamente essere utilizzati per prevedere dove è più probabile che si verifichino gli abusi di droga[187].

Naturalmente, molte persone innocenti con il raffreddore, potrebbero comprare questo articolo, di per sé legale[188].

La correlazione, quindi, sebbene sia sospetta, non è criminale. E questo solleva la questione fondamentale legata all'indagine algoritmica, ossia quella sulla concreta affidabilità degli algoritmi[189].

David Vladeck, l'ex direttore del *Bureau of Consumer Protection* presso la *Federal Trade Commission* ha chiarito: "Gli algoritmi possono anche essere strumenti decisionali imperfetti. Gli algoritmi sono progettati dagli esseri umani, e, per questo, lasciano aperta la possibilità che errori umani, difficilmente riscontrabili, relativi alla fase di programmazione del sistema possano contaminare la pratica. E gli algoritmi non sono migliori dei dati che elaborano, e sappiamo che molti di quei dati possono essere inaffidabili, obsoleti o riflettere pregiudizi[190]".

Gli algoritmi, quindi, possono anche sbagliare. Pedro Domingos, professore di informatica all'Università di Washington e autore di "*The Master Algorithm*", ha illustrato come l'apprendimento automatico possa sbagliare[191]".

In un articolo del *Washington Post*, ha spiegato il funzionamento di un algoritmo informatico ideato per chiarire la differenza tra lupi e cani

---

[186]Cfr., TALBERT Jeffery et al., *Pseudoephedrine Sales and Seizures of Clandestine Methamphetamine Laboratories in Kentucky*, in *JAMA* 2012, 1524, 308; BARDIN Jon, *Kentucky Study Links Pseudoephedrine Sales, Meth Busts*, in *L.A. TIMES*, 2012.

[187]Cfr., FERGUSON Andrew Guthrie, *Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards*, in *OKLA*, 2014, 831-841, 66.

[188]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 118 s.

[189]*Ibidem.*

[190]Cfr., VLADECK David C., *Consumer Protection in an Era of Big Data Analytics*, in *OHIO N.U.* 2016, 493-495, 42.

[191]Cfr., DOMINGOS Pedro, *The master algorithm: how the quest for the ultimate learning machine will remake our world*, 2015.

selvatici[192]". Durante il test, l'algoritmo ha funzionato perfettamente, troppo perfettamente. Solo dopo un'ulteriore ispezione è stato rivelato il perché, mostrando una perfezione solo apparente. Tutte le foto dei lupi erano state scattate con la neve bianca sullo sfondo, e nessuna delle foto dei cani aveva la neve sullo sfondo. Il computer aveva semplicemente imparato ad associale la neve ai lupi"[193]. Pericoli simili sono legati agli algoritmi predittivi; i falsi ‘’*flag’’* potrebbero dimostrare talune correlazioni erronee a causa di un modello mal progettato[194].

La tecnologia del *data mining* può essere applicata anche ai dati relativi ai social media. La polizia di Austin, Oakland, San Diego, San Jose, Santa Clara e Philadelphia ha sperimentato ‘’*Geofeedia*’’[195], un *software* che consente agli utenti di taggare, cercare e ordinare i contenuti dei social media a fini investigativi[196].

Le possibilità, di indagare tramite i *social media*, sono molto utili per la polizia. Si immagini, ad esempio, che, pochi istanti dopo una sparatoria in un club, la polizia usi uno strumento simile a *Geofeedia* per isolare l'area geografica intorno al club e cercare tutti i post di *Twitter, Facebook, Instagram, Picasa* e *Flickr* in tempo reale[197].

Il funzionamento del *software* è basato sulla ricerca di commenti pubblici tramite parole chiave, come "pistola", "sospetti", e le associa alla geo-localizzazione dell’individuo che ha pubblicato il commento[198]. Le comunicazioni tra gli individui potrebbero essere collegate, così, in modo da trovare quelli eventualmente presenti sulla scena del crimine tramite video o

---

[192]Cfr., MCFARLAND Matt, *Terrorist or Pedophile? This Start-Up Says It Can Out Secrets by Analyzing Faces,* in *WASH. POST*, 2016.

[193]*Ibidem.*

[194]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 121.

[195]Cfr., CANTÚ Aaron, *#Followed: How Police across the Country Are Employing Social Media Surveillance*, in *MUCKROCK*, 2016.

[196]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 114.

[197]*Ibidem.*

[198]*Ibidem.*

foto pubblicati[199]. La polizia potrebbe creare un *database* con tutti i *post* condivisi in rete collegandoli al luogo del delitto[200].

La sorveglianza dei *social media* può anche aiutare la polizia a indagare sulle aree ad alta criminalità, ad esempio, intercettando tutti i *post* provenienti da quella particolare area geografica[201]. Il risultato è la creazione di un programma di sorveglianza capace di monitorare le attività digitali ed eventualmente scoprire minacce o commenti presenti sul *web* che suggeriscono attività criminali.

Gli accademici hanno anche iniziato a studiare Twitter per prevedere e prevenire il crimine. *Twitter*, infatti, è un *social* creato per condividere le proprie idee, rappresenta, quindi, le opinioni attuali della società, e quindi potrebbe essere utile per identificare i rischi futuri della violenza[202].

In un'intervista con *NPR's All Things Considered*, Desmond Patton, professore della *Columbia University*, ha spiegato come è riuscito a sviluppare un algoritmo volto ad estrarre i *tweet* per prevedere la violenza: "Sull'idea che se possiamo esaminare il tono del linguaggio, utilizzato nei tweet, si possono prevedere i comportamenti futuri degli individui, quindi possono essere attivate azioni preventive come inviare presso le loro abitazioni assistenti sociali in modo che possano utilizzare le strategie per prevenire il crimine[203]''.

Resta problematica la questione della *privacy*, come nel caso dei metadati[204], poiché per monitorare i rischi individualizzati la polizia finisce per raccogliere i dati di tutti, anche dei cittadini innocenti che subirebbero una lesione ingiusta della loro sfera personale.

5. La problematica della mancanza di dati

[199]*Ibidem.*

[200]Cfr., GOLDSTEIN Joseph e GOODMAN J. David, *Seeking Clues to Gangs and Crime, Detectives Monitor Internet Rap Videos*, in *N.Y. TIMES*, 2014.

[201]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 115.

[202]*Ibidem.*

[203]Cfr., CORLEY Cheryl, *When Social Media Fuels Gang Violence, all tech considered* in *NPR radio broadcast*, 2015.

[204]V. paragrafo 3. I Metadati.

Gran parte della raccolta di dati, tramite i sistemi di analisi dei *big data*, comporta la loro acquisizione digitale attraverso dispositivi elettronici personali (*social-media mining*, metadati). Quando d'altro canto, questo accesso ai dati è precluso, il risultato è non avere alcuna traccia di dati. Mentre la società si muove verso un sistema di polizia sempre più dipendente dalla tecnologia dei *big data*, colmare queste lacune di dati o, come minimo, riconoscerne l'esistenza è essenziale, per evitare di effettuare indagini incomplete o inefficaci[205].

La mancanza di dati è relativa, soprattutto, ad alcune categorie di cittadini che vivono ai margini della società (situazioni di povertà, senzatetto, disoccupati) o che esercitano attività criminali, nascondendosi volontariamente dalla tecnologia dei *big data*.

Chi non possiede uno *smartphone*, non fa acquisti online, non usa la carta di credito, non è in possesso di un'auto o addirittura non ha un indirizzo di casa, resta quasi del tutto nascosto dalla raccolta dei *big data*[206].

Come ha riconosciuto Kate Crawford, ''non tutti i dati vengono raccolti allo stesso modo, ci sono zone oscure o ombre nei grandi set di dati, con la conseguenza che alcuni cittadini sono trascurati o sottorappresentati''[207]. Jonas Lerman ha aggiunto: "La realtà è che miliardi di persone rimangono ai suoi margini perché non si impegnano abitualmente in attività che i big data e l'analisi avanzata sono progettati per catturare"[208].

L'esclusione delle persone povere e di quelle ai margini della società dai *set* di dati raccolti pone implicazioni problematiche per l'egualitaria opportunità economica, per la mobilità sociale e la partecipazione democratica

[205]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 178.

[206]*Ibidem.*

[207]Cfr., CRAWFORD Kate, *Think Again: Big Data*, in *FP*, 2013, *www.foreignpolicy.com.*

[208]Cfr., LERMAN Jonas, *Big Data and Its Exclusions*, in *STAN.* 2013, 55-56, 66.

di tutti i cittadini nella società[209]. I soggetti invisibili ai *big data* possono essere dimenticati da un sistema dipendente da esso[210].

Dal punto di vista economico, i *broker* di dati dei consumatori non hanno un incentivo finanziario tale da ottenere con certezza assoluta dati corretti. I *broker* di dati dei consumatori prosperano vendendo informazioni alle aziende[211]. Le persone ai margini del sistema economico non meritano il tempo e l'energia necessari per acquisire buoni dati. Ciò non significa che le aziende potrebbero non avere alcune informazioni su ogni indirizzo di casa o persona, ma il livello di dettaglio e quindi l'accuratezza potrebbero essere inferiori.

Se la polizia inizia a dipendere dalle aziende private di analisi dei *big data* per basare le valutazioni del ‘’rischio’’ di criminalità, allora tale imprecisione applicata ai quartieri poveri, e alle aree ad alto rischio di delinquenza, potrebbe condurre ad una mappatura del crimine errata, producendo risultati investigativi inattendibili[212].

Come aggravante, coloro che sono più a rischio di attività criminali non saranno facilmente riscontrabili nei sistemi di *big data* che analizzano consumatori; ciò si tradurrebbe, paradossalmente, in un beneficio per gli attori criminali che cercano di nascondersi dalla sorveglianza del governo.

Altrettanto problematica, è la raccolta di dati inerenti ad alcuni crimini regolarmente non denunciati[213].È il caso di abusi fisici e sessuali interfamiliari che non vengono segnalati a causa delle relazioni personali coinvolte o della tossicodipendenza[214]. La violenza sessuale resta spesso nell’ombra a causa

[209]Cfr., LERMAN Jonas, *Big Data and Its Exclusions*, in *STAN.* 2013, 55-56, 66.

[210]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 179.

[211]Cfr., JEROME Joseph W., *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, in *STAN*, 2013, 47-50, 66.

[212]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 179.

[213]Cfr., Comunicato stampa, *Bureau of Justice Statistics, U.S. Dep't of Justice, Office of Justice Programs, Nearly 3.4 Million Violent Crimes per Year Went Unreported to Police 2006-2010*, 2012, available at *www.bjs.gov*.

[214]Cfr., CAREY Camille & SOLOMON Robert A., *Impossible Choices: Balancing Safety and Security in Domestic Violence Representation*, in *CLINICAL*, 2014, 201-225, 21; SUK Jeannie, *Criminal Law Comes Home*, in *YALE*, 2006, 2, 15-16, 116.

dello stigma sociale e delle difficoltà legali di segnalazione[215], la maggior parte dei tossicodipendenti non si auto-segnalo, sussiste poi il problema della difficoltà investigativa legata ai *''White collarcrimes''*.

Purtroppo, talvolta, anche i crimini violenti sfuggono ai sistemi di *big data*[216].Il *Bureau of Justice Statistics* ha scoperto che quasi la metà dei crimini violenti (3,4 milioni di incidenti all'anno) non vengono segnalati[217]. Parallelamente alle altre ragioni, lo studio della *BJR* ha rilevato che le vittime di crimini violenti hanno esporto denuncia o per timore o perché conoscevano l'autore del reato o perché ''hanno preferito gestire la situazione in modo diverso[218] ''.

La combinazione di lacune legate alla classe sociale o a taluni settori criminali, ha dato vita un sistema di polizia di big data che aveva successo solo sulla metà dei dati tracciati sulla criminalità[219]. Tale distorsione si traduce in una parziale inaffidabilità delle tecnologie basate sull'analisi dati e può dare luce ad una falsa visione di successo del sistema.

D'altro canto, alcuni crimini come omicidi, aggressioni sessuali, reati contro il patrimonio (come furti d'auto e furti con scasso) e altri crimini con lesioni gravi tendono ad essere segnalati dalle vittime e tracciati dai *big data* in modo abbastanza accurato[220].In questi casi, la dipendenza della polizia dai sistemi basati sui dati ha una effettiva ragionevolezza.

Alla fine di questa analisi, è possibile affermare che i *''data holes''* non sono ovunque, ma rappresentano spazi di oscurità nel sistema della tecnologia dei *big data* che devono essere quantomeno riconosciuti, onde evitare l'affidamento delle forze dell'ordine ad analisi inaccurate.

---

[215]Cfr., HELD Myka & MCLAUGHLIN Juliana, *Rape & Sexual Assault*, in *GENDER GEO. J. & L.*, 2014, 155-157, 15.

[216]Cfr., Comunicato stampa, *Bureau of Justice Statistics, U.S. Dep't of Justice, Office of Justice Programs, Nearly 3.4 Million Violent Crimes per Year Went Unreported to Police 2006-2010*, 2012, available at *www.bjs.gov*.

[217]*Ibidem.*

[218]*Ibidem.*

[219]Cfr. FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 181.

[220]Cfr., FERGUSON Andrew Guthrie, *Predictive Policing and Reasonable Suspicion*, in *EMORY* , 2012, 259 -317, 62.

Elizabeth Joh, un'esperta di sorveglianza basata sui *big data*, ha chiarito che la mancanza dei dati spesso deriva dal fenomeno della c.d. "*privacy protest*"[221].

I cittadini vedono violata la propria privacy per cui reagiscono alla sorveglianza dei *big data* nascondendo o protestando contro il monitoraggio pervasivo. Con l'utilizzo della tecnologia, cercano di evadere il riconoscimento facciale, di eludere i lettori di targhe e si nascondono dalla sorveglianza elettronica[222]. Ci sono linee di abbigliamento antidrone o orologi-radar che intercettano dispositivi di registrazione audio nelle vicinanze[223].

Anche i criminali, al pari dei cittadini, sanno come eludere la sorveglianza della polizia: se le automobili sono monitorate attraverso *ALPR*, gli autori degli illeciti smetteranno di usare le proprie auto; se i cellulari vengono intercettati, i criminali useranno telefoni usa e getta[224].

Infine, i sostenitori della privacy possono organizzarsi contro la raccolta di dati in determinate aree.

Ad esempio, le proteste della comunità contro i voli dei droni a Seattle ne hanno interrotto l'uso da parte della polizia[225]. Lo stesso è accaduto ad Oakland ove serrate opposizioni hanno impedito l'adozione della polizia predittiva, nonché a Baltimora relativamente all'uso di sistemi di sorveglianza persistenti[226].

Il risultato di tutto ciò è che, nelle aree geografiche più organizzate alla protesta saranno catturati meno dati rispetto alle comunità meno organizzate (che, in genere sono le più povere), e ciò causerà ulteriore iniquità nella raccolta e nell'uso dei dati.

---

[221]Cfr., JOH Elizabeth E., *Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion*, in *ARIZ.*, 2013, 997-1002, 55.

[222]*Ibidem.*

[223]Cfr., MALY Tim, *Anti-Drone Camouflage: What to Wear in Total Surveillance*, in *WIRED*, 2013, *www.wired.com*.

[224]Cfr., FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017, 184.

[225]Cfr., CLARRIDGE Christine, *Protesters Steal the Show at Seattle Police Gathering to Explain Intended Use of Drones*, in *SEATTLE TIMES*, 2012.

[226]Cfr., WHEELER Brian, *Police Surveillance: The US City That Beat Big Brother*, in *BBC NEWS MAG.*, 2016, *www.bbc.com.*

6. La fallibilità dei dati

Anche se correttamente raccolti e archiviati, i dati possono essere successivamente soggetti a vizi materiali o interpretativi a causa dell'errore umano da parte dei tecnici informatici in sede di programmazione degli algoritmi predittivi[227]. Oltre ciò, frequentemente vengono caricati profili DNA non autorizzati dalla legge (ad es. quelli delle vittime) che anziché essere cancellato o distrutti, vengono conservati e utilizzati dai governi nelle indagini successive[228].

Ricorrenti sono ad esempio numeri di previdenza sociale errati, nomi imprecisi e "date di nascita illogiche" che comunemente inducono all'errore giudiziario e provocano arresti ingiusti[229]. Nel 2011, il Los Angeles Times ha riferito che nei cinque anni precedenti, mandati infondati hanno portato all'arresto illegale di quasi 1500 persone nella contea di Los Angeles, con detenzioni ingiuste di circa tre settimane per ogni arrestato[230].

Studi statistici sulla giustizia hanno evidenziato che nei casellari giudiziari sono inseriti molti documenti contenenti informazioni incomplete e imprecise o addirittura inesatte e che oltre un quarto degli Stati esaminati non hanno rispettato uno o entrambi i requisiti federali, che prevedevano che i *database* dei registri contenessero tutte le informazioni note sugli arresti e che detti arresti fossero comunicati all'*FBI* entro 120 giorni dal verificarsi dell'arresto[231].Circa il cinquanta per cento dei documenti mancava di

---

[227]Cfr., GOLDSTEIN Joseph, *F.B.I. Audit of Database That Indexes DNA Finds Errors in Profiles,* in *N.Y. TIMES*, 2014, at A15; HSU Spencer S., *FBI No- tifies Crime Labs of Errors in DNA Match Calculations Since 1999*, in *WASH. POST*, 2015.

[228]Cfr., LOGAN Wayne A., *Government Retention and Use of Unlawfully Se- cured DNA Evidence*, in *TEX. TECH*, 2015, 269-280, 48.

[229]Cfr., PITTS Wayne J., *From the Benches and Trenches: Dealing with Out- standing Warrants for Deceased Individuals: A Research Brief*, in *JUST. SYS. J.*, 2009, 219-220, 30.

[230]Cfr., LOGAN Wayne A. & FERGUSON Andrew Guthrie, *Policing Criminal Justice Data,* in FSU COLLEGE OF LAW (diretto da), Minnesota, 2016 , Law Review 541, Research Paper n. 799, 559.

[231]Cfr., U.S. GOV'T. ACCOUNTABILITY OFFICE GAO-15-162, REPORT TO CONGRESSIONAL REQUESTERS: *CRIMINAL HISTORY RECORDS: ADDITIONAL ACTIONS COULD ENHANCE THE COMPLETENESS OF RECORDS USED FOR EMPLOYMENT- RELATED BACKGROUND CHECKS* 25 (Feb. 2015), *http://gao.gov/assets/670/ 668505.pdf. States are permitted ninety days to gather and complete disposi- tion records for own their central repositories.* 28 C.F.R. § 20.21(a)(1). *Before being required to report to the FBI, states*

informazioni riguardanti la sentenza definitiva del caso[232]. I registri degli autori di reati sessuali sono pieni di errori, soprattutto per quanto riguarda le informazioni sull'indirizzo di casa[233]. Anche i *database*, relativi alle bande criminali, contengono molti errori[234], come ad esempio rapporti non corrispondenti[235],segnalazione di documenti sigillati o cancellati[236], disposizioni incomplete[237], e mancata classificazione corretta degli incidenti, insomma mancata corrispondenza alla realtà di fatti e persone.

Per gli individui, l'errore relativo all'analisi dei dati può avere conseguenze problematiche. Un individuo nei cui confronti è stato emesso un mandato di arresto, vede limitata enormemente la propria libertà fisica, venendo altresì violata la propria privacy. Subisce, infatti, perquisizioni personali, viene perquisita la sua casa, la sua auto, è costretto a lasciare la propria casa, i propri affetti, oltre che a subire una ingiusta detenzione e rimanerci anche per molti giorni, o per tutto il tempo necessario affinché venga riconosciuto l'errore giudiziario.

Un ulteriore problema nasce dal fatto che qualora l'individuo, erroneamente arrestato, non abbia i soldi per pagare la cauzione - un evento comune anche quando è fissato a un importo basso –è costretto a subire la

---

are given an extra thirty days, "to allow for processing time that may be needed by the states before forwarding the disposition." 28 C.F.R. app. pt. 20.

[232]Cfr., LOGAN Wayne A. & FERGUSON Andrew Guthrie, *Policing Criminal Justice Data,* in FSU COLLEGE OF LAW (diretto da), Minnesota 2016, Law Review 541, Research Paper N. 799, 561.

[233]Cfr., U.S. DEP'T OF JUSTICE, EVALUATIONS & INSPECTIONS DIV., I- 2009-001, REVIEW OF THE DEPARTMENT OF JUSTICE'S IMPLEMENTATION OF THE SEX OFFENDER REGISTRATION AND NOTIFICATION ACT, v–vi (Dec. 2008) (noting widespread inaccuracies in state registry information); SHEEHAN Charles, *Sex Offenders Slip Away*, CHI. TRIB., 2006, *http://articles .chicagotribune.com/2006-03-31/news/0603310164_1_number-of-sex-offenders* -parole-illinois-prisoner-review-board (noting that in Chicago over seventy-five percent of randomly sampled addresses of registrants were invalid); *see also* Press Release, *Kansas Office of the Attorney Gen., Attorney General Kline Re- leases Results of Kansas Sex Offender Registry Audit*, 2005, *http://cdm16884 .contentdm.oclc.org/cdm/singleitem/collection/p16884coll31/id/151/rec/12*.

[234]Cfr., MITNICK Eric. J., *Procedural Due Process and Reputational Harm: Liberty as Self-Invention*, in *U.C. DAVIS*, 2009, 79-126, 43; WRIGHT Joshua D., *The Constitutional Failure of Gang Databases*, in *STAN. J. C.R. & C.L.*, 2005, 115, 119-29, 2; v. anche HOBSON Will, *Overhaul Coming to Pinellas Gang Intelligence Database*, in *TAMPA BAY TIME*, 2013, *http://www.tampabay .com/news/courts/criminal/overhaul-coming-to-pinellas-gang-intelligence -database/2125725.*

[235]Cfr., YU PERSIS S. & DIETRICH SHARON M., *nat'l consumer law ctr., broken records: how errors by criminal background checking companies harm workers and businesses,* 2012, 7 e 20.

[236]*Ivi,* 20 e 23.

[237]*Ivi,* 24 e 26.

detenzione per diversi giorni[238], o fino a quando il sistema giudiziario non riconosca l'errore[239].L'arresto può anche avere importanti conseguenze sulla sua reputazione.

Servizi come ArrestWarrants.org, che si basa su "dati ufficiali da database pubblici e privati", pubblicano notizie e "foto segnaletiche" sulle pagine web dei dipartimenti di polizia[240] , dei giornali[241], sui siti web gestiti da imprese commerciali[242]. A causa di ciò, poiché a questi dati hanno accesso tutti i cittadini, attraverso un computer, un arresto viene conosciuto da chiunque e tale notizia può influire negativamente, sulla ricerca di un alloggio, di una occupazione, di un prestito; e ciò perché essere arrestato, nella opinione pubblica, equivale a essere coinvolti in attività criminali[243].

Inoltre, successivamente al rilascio, nel suo *database* personale non viene annotato quale reato gli sia stato attribuito, per cui l'opinione pubblica può anche pensare che fosse un assassino.

La ricercatrice Amy Myrick ha condotto un lavoro sul campo durato un anno che ha esaminato le fedine penali di oltre centocinquanta adulti che, avendo subito delle accuse penali infondate, hanno chiesto la cancellazione dai propri documenti delle notizie sbagliate.

Myrick ha anche rilevato molti casi in cui le identità registrate delle persone sono state fuse "quando i documenti del tribunale hanno attribuito un caso alla persona sbagliata, fondendo così le loro storie", causando in molti casi un errore di identità[244].

---

[238]Cfr., SZPALLER Keila, *City of Missoula Makes Wrongful Arrests on Invalid Warrants*, in *Missoulian*, Missoula, 2013.

[239]Cfr., *Invalid 1989 Arrest Warrant Detours Ike Turner for Night*, in *TIMES UNION*, Albany, N.Y., 2007.

[240]Cfr., BIDGOOD Jess, *After Arrests, Quandary for Police on Posting Booking Photos*, in *N.Y. TIMES* , 2015.

[241]Cfr., *Mugshots Gainesville*, in *GAINSVILLE SUN*,, 2016, *http:// mugshotsgainesville.com.*

[242]Cfr., LOGAN Wayne A. & FERGUSON Andrew Guthrie., *Policing Criminal Justice Data*, in FSU COLLEGE OF LAW (diretto da), Minnesota 2016, Law Review 541, Research Paper N. 799, 565.

[243]Cfr., Illinois v. Gates, in *U.S.*, 1983, 213-246, 462; v. anche Wilson v. Russo, in *F.3d*, 3d, Cir. 2000, 781-789, 212.

[244]Cfr., MYRICK Amy, *Facing Your Criminal Record: Expungement and the Col- lateral Problem of Wrongfully Represented Self*, in *L. & SOC'Y* , 2013, 73, 47, 91.

Di tutto ciò i cittadini nella maggior parte dei casi, non sanno nulla per cui la Myrick ha concluso la sua indagine affermando che un casellario giudiziario è "un materiale delega che l'ordinamento giuridico ha composto alle sue condizioni, che può rimanere imperscrutabile e persino sconosciuto ai soggetti in esso registrati[245], che però sono presi di mira dalla polizia e dalla società, subendo gravissimi danni personali, per essere stati inseriti nei casellari giudiziari o per aver subito un arresto ingiusto, a causa di un errore del database.

Oltre ciò, gli stessi mandati di arresto, come ha recentemente osservato il giudice Kagan, non sono distribuiti uniformemente nella popolazione, essendo concentrati in aree specifiche. Uno studio ha rilevato, ad esempio, che Cincinnati, Ohio, aveva oltre 100.000 mandati di arresto con soli 300.000 residenti[246]. Come osserva, invece, il giudice Sotomayor, 16.000 delle 21.000 persone residenti nella città di Ferguson, Missouri hanno mandati pendenti[247].Gli errori nei dati possono quindi avere un impatto disparato sulla minoranza povera, che spesso subisce svantaggi comparativi nell'individuare e contestare documenti inesatti.

Se gli errori dei dati, come abbiamo visto, danneggiano le persone coinvolte in errori giudiziari, è pur vero che possono avere significative implicazioni negative anche per i governi che hanno ovviamente il dovere di garantire e tutelare in modo scrupoloso, la libertà, la privacy e altri interessi dei suoi cittadini[248], oltre che garantire la efficienza della polizia e degli uffici giudiziarie di intelligence a ciò preposti.

---

[245]*Ivi,* 102.

[246]Cfr., LOGAN Wayne A. & FERGUSON Andrew Guthrie., *Policing Criminal Justice Data,* in FSU COLLEGE OF LAW (diretto da), Minnesota 2016, Law Review 541, Research Paper N. 799, 568.

[247]Cfr., Utah v. Strieff, 136 S. Ct. 2056, 2073 n.1 (2016) (KAGAN, J., dissenting); CIVIL RIGHTS DIV., U.S. DEP'T OF JUSTICE, INVESTIGATION OF THE FERGUSON POLICE DEPARTMENT 3–4 (2015), *https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_ report.pdf*. For further discussion of the tendency of governments to utilize the criminal justice system to generate revenues, see LOGAN Wayne A. &WRIGHT Ronald F., *Mercenary Criminal Justice,* 2014, 1175.

[248]Cfr., *Cf. Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics,* in *U.S.,* 1971, 388-392, 403.

Gli errori dei data base minano la fiducia nello Stato e mettono in discussione la competenza e l'equità del governo[249]. Quando un individuo viene erroneamente preso di mira dalla polizia ingiustificatamente o subisce un ingiusto mandato d'arresto, non solo subisce dei danni, ma prende atto del fatto che le risorse di polizia, correzionali e giudiziarie non sono ben organizzate se non addirittura inefficienti[250]. Se un individuo scopre che un dato sbagliato che lo riguarda non è stato cancellato; se accerta che nella raccolta dei dati ci sono innumerevoli notizie sbagliate o inesatte che sovraccaricano il sistema, non giustifica lo Stato da cui si aspetta totale efficienza e tutela, ma perde fiducia nelle istituzioni e, soprattutto nella validità della raccolta dei dati che, quando è elaborata in maniera imprecisa, fa incorrere nell'errore giudiziario e rende inefficiente l'attività di prevenzione dei reati[251].

7. La sistematica degli algoritmi predittivi

Attualmente i giudici, nella valutazione della pericolosità criminale, e cioè nell'esaminare se un individuo, con determinate caratteristiche, sia predisposto per il futuro a commettere uno o nuovi reati –indagine necessaria quando si tratta, ad esempio, di applicare una misura di sicurezza, cautelare o di prevenzione – si affidano esclusivamente alla loro esperienza personale, al loro buon senso.

Nell'immediato futuro, queste valutazioni sulla pericolosità criminale, di tipo meramente intuitivo, potrebbero essere affidate a specifici algoritmi (i *risk assessment tools*, algoritmi predittivi, già attualmente applicati in altri ordinamenti giuridici)capaci di attingere e rielaborare quantità enormi di dati al fine di far emergere relazioni, coincidenze, correlazioni, che consentano di

[249]Cfr., SHANE Peter M., *The Bureaucratic Due Process of Government Watch Lists*, in *GEO. WASH.*, 2007, 804-808, 75. For discussion of the critical role police play more generally in upholding rule of law values and instilling public trust, and the negative consequences of failing at the enterprise, see LOGAN Wayne A., *Police Mistakes of Law*, in *EMORY*, 2011, 69-90–92, 61.

[250]Cfr., LOGAN Wayne A. & FERGUSON Andrew Guthrie., *Policing Criminal Justice Data*, in FSU COLLEGE OF LAW (diretto da), Minnesota 2016, Law Review 541, Research Paper N. 799, 571.

[251]*Ibidem.*

creare lo screening della personalità di taluni soggetti a ‘’rischio’’ e prevederne i successivi comportamenti, anche di rilevanza penale[252].

Grazie a questi algoritmi, la valutazione della pericolosità sociale di un individuo, non sarà il frutto di una valutazione meramente intuitiva, ma di una valutazione “attuariale” (statistica) che costituisce il presupposto teorico degli algoritmi predittivi, basata su riscontri oggettivi, destinata a sostituire, o quanto meno integrare, le valutazioni discrezionali dei giudici, tuttora ampiamente diffuse.

La pericolosità di un individuo, ricercata tramite il metodo *‘’evidence-based*’’[253] (valutazione del rischio individuale di commissione di un nuovo reato), sarà basata su riscontri oggettivi, previa la individuazione di una serie di fattori di rischio (o predittivi) quale ‘’il sesso, l’origine etnica, il livello di scolarizzazione, la situazione familiare e lavorativa, la posizione sociale, i precedenti penali, le precedenti esperienze carcerarie, i luoghi e le persone frequentati, la presenza di autori di reato nella cerchia familiare o nella rete di conoscenze, il luogo di residenza, le difficoltà di regolazione della rabbia e dell’aggressività, il cattivo controllo degli impulsi, una storia di precedente violenza, una storia di ospedalizzazione, un pensiero pro-criminale, alcune variabili contestuali (quali, ad esempio, la mancanza di sostegno familiare e sociale), il consumo di sostanze stupefacenti o alcoliche, possono condizionare il comportamento criminoso o condurre alla commissione di un nuovo reato’’[254].

Tutti questi fattori, una volta raccolti, grazie a studi longitudinali prospettici, vengono combinati tra di loro e, consentendo, su base statistica, di

[252]Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 16.

[253]Cfr., ZARA Georgia, *Tra il probabile e il certo.* La valutazione dei rischi di violenza e di recidiva criminale, in Diritto penale contemporaneo, 20 maggio 2016, con riferimento, in particolare, al lavoro di SINGH J. P. et al., *A comparative study of violence risk assessment tools: a systematic review and meta-regression analysis of 8 studies involving 25980 participants, in Clin Psychol Rev,* 31, 2011, pp. 499 ss.

[254]Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 17.

predisporre delle c.d. ‘‘scale’’ che attribuiscono un punteggio di pericolosità (score) al soggetto preso in esame[255].

Le “scale” vengono elaborate in base alla popolazione (ad esempio, popolazione di adulti, di minori, di maschi, di femmine, di pazienti psichiatrico-forensi, di detenuti o ex-detenuti); in base alla tipologia di reati(esistono scale generiche, cioè relative a tutti i reati, e scale specifiche, relative a singole tipologie di reati, come i reati sessuali o i reati violenti); in base alla ‘’temporalizzazione”[256] del rischio (immediato, o a medio o a lungo termine); in base, infine, al contesto (comunità civile, istituti di pena, centri di salute mentale, ospedali psichiatrico-giudiziari).

Una volta elaborate, le informazioni vengono utilizzate per la valutazione statistica ‘’attuariale’’[257] della pericolosità criminale, in base ai fattori di rischio che non sono tutti uguali e si distinguono in base al loro differente tasso di dinamicità[258]. Esistono, infatti: i) fattori statici, ossia quei fattori non modificabili, come, ad esempio, il sesso e l’origine etnica; ii) fattori dinamici stabili, fattori modificabili grazie al trattamento terapeutico, come, ad esempio, lo scarso controllo degli impulsi; iii) fattori di rischio acuti, che riguardano condizioni che facilitano o agevolano la reazione violenta, come, ad esempio, l’uso di sostanze stupefacenti[259].

Naturalmente, più numerosi sono i fattori di rischio, più alta sarà la probabilità di commissione di reati (*outcomes*). Si tratta della c.d. *dose-exposure relation ship*: «precocità, durata e intensità dell’esposizione a più fattori di rischio che interagiscono in modo cumulativo, aumentando la probabilità di violenza e manifestazioni criminali»[260] .

---

[255]Cfr., CASTELLETTI L., RIVELLINI G., STRATICÒ E., *Efficacia predittiva degli strumenti di ViolenceRiskAssessment e possibili ambiti applicativi nella psichiatria forense e generale italiana,* in *Journal of Psychopathology*, 2014, 153 ss.; CANDELLI C., CARABELLESE F., ROCCA G., ROSSETTO I., *La valutazione psichiatrico forense della pericolosità sociale del sofferente psichico autore di reato: nuove prospettive tra indagine clinica e sistemi attuariali,* in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario),* 2012, n. 4, 1442 ss., 18.

[256]Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 18.

[257]*Ibidem.*

[258]*Ibidem.*

[259]Cfr., ZARA G., *Tra il probabile e il certo,* cit., 12.

[260]Cfr., ZARA G., *Tra il probabile e il certo,* cit., 17 ss.

Negli Stati Uniti, queste valutazioni attuariali vengono affidate, a sistemi di intelligenza artificiale, quindi ad algoritmi predittivi di pericolosità criminale, basati su procedure di autoapprendimento[261] (*machine learning*) e straordinaria capacità e rapidità di riconoscere relazioni, coincidenze, correlazioni. I vantaggi sono enormi, così come, purtroppo, i rischi legati all'uso incontrollato delle IA.

Gli algoritmi predittivi sono applicati, altresì, per decidere se un individuo, nelle more della celebrazione del processo, possa essere rilasciato dietro il pagamento di una eventuale cauzione, o per misurare il rischio di recidiva del condannato, per valutare se sia ammissibile la libertà vigilata o altra misura alternativa alla detenzione.[262]

Due sono gli algoritmi di valutazione di pericolosità criminale introdotti negli Stati Uniti.

Il primo, denominato *PUBLIC SAFETY ASSESSMENT*(PSA), ideato da una organizzazione non profit (la "*Laura and John Arnold Foundation*"), nasce col proposito di aiutare i giudici a formulare una prognosi criminale, tramite indicazioni scientifiche in tempi rapidi[263].

Il secondo, più celebre, chiamato *COMPAS –Correctional Offender Management Profiling for Alternative Sanctions,* è un *software* elaborato e commercializzato da una società privata, la *Northpointe* (da gennaio 2017, ridenominata *Equivant*)[264].

L'algoritmo *PSA* è capace di mettere a confronto vari fattori di misurazione del rischio (sono nove tra cui l'età, i precedenti penali, le comparizioni in tribunale e le denunce ricevute in casi precedenti, non compaiono né la razza, né l'origine etnica e geografica[265])di un determinato

[261]Cfr., ZARA G., *Tra il probabile e il certo,* cit., 14.

[262]Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 18.

[263]Cfr. LIVNI E., *Nei tribunali del New Jersey è un algoritmo a decidere chi esce su cauzione,* in *Internazionale,* 2017 (trad. FERRONE F.).

[264]Cfr., DRESSEL J., FARID H., *The accuracy, fairness, and limits of predicting recidivism,* in *Science Advances,* 2018, fasc. 4, 1 ss.: gli Autori riportano stime dalle quali risulterebbe che COMPAS, da quando è stato sviluppato nel 1998, è stato utilizzato in più di un milione di casi.

[265]Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 18.

soggetto, e con l'ausilio di un database di 1,5 milioni di casi provenienti da trecento giurisdizioni di tutti gli Stati Uniti, e in base alle informazioni a disposizione, attribuisce al medesimo individuo un punteggio di pericolosità su una scala da uno a sei.[266]

Il *PSA* è stato adottato nello Stato del New Jersey e, da allora, è aumentato vertiginosamente il numero delle persone rilasciate su ''*parole*''[267], in particolare c'è stato un incremento di quelle rilasciate senza il pagamento di una cauzione. Dall'indagine emerge che gli algoritmi utilizzati nel passato avessero favorito i soggetti non-pericolosi e non abbienti. Uno studio del 2013 aveva, infatti, messo in evidenza che quasi il 40 % degli imputati restava in prigione a causa di una situazione economica tale da non poter pagare la cauzione. Grazie al *PSA*, software che fornisce una valutazione ''neutrale'', indipendente dalla situazione economica, oggi gli imputati sono rilasciati, sulla base della loro idoneità alla messa in libertà (valutazione che, tuttavia, si affianca a quella del giudice, senza sostituirla).[268]

L'algoritmo *COMPAS*, invece, è uno strumento che compie una valutazione sui rischi di commissione di un reato, e delle relative esigenze trattamentali[269]. Le agenzie di giustizia penale utilizzano *COMPAS* per assumere decisioni in merito al collocamento, alla supervisione e alla gestione degli autori di reati[270].

COMPAS è stato sviluppato prendendo in considerazione i fattori di rischio statici e dinamici e fornisce informazioni, ampiamente convalidate sulla base di ricerche scientifiche, su tali fattori, al fine di agevolare gli interventi correttivi volti a ridurre le probabilità di recidiva[271]. Tale sistema è stato utilizzato per la prima volta nel 1998 e viene periodicamente aggiornato per

[266]*Ibidem.*

[267]*Ibidem.*

[268]Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 19.

[269]*Ibidem.*

[270]*Ibidem.*

[271]*Ibidem.*

evolvere continuamente e incrementare la certezza dei risultati delle sue analisi, stando al passo con le nuove pratiche emergenti e i progressi tecnologici[272].

COMPAS, nella sua versione di base, risponde a 137 quesiti riguardanti: precedenti criminali o illeciti o infrazioni, l'eventuale passato o presente di violenza, frequentazioni con criminali, abuso di sostanze, problemi economici, difficoltà nell'istruzione e nella formazione professionale, ambiente familiare delinquenziale, contesto sociale, modo di utilizzo del tempo libero, instabilità residenziale, adeguamento sociale, difetti di socializzazione, opportunità criminali, isolamento sociale, pensiero pro-criminale, personalità criminale[273]. Sulla base di questi indicatori vengono elaborate alcune risposte sulla pericolosità o meno del soggetto oggetto dell'analisi, anche a mezzo di ricerca presso archivi o registri a disposizione delle procure e della polizia. Tra i fattori esaminati non rientra la razza.

In sede di interrogatorio con l'imputato il *software* aiuta i pubblici ministeri o la polizia giudiziaria a porre alcune domande come, ad esempio, chiedere se i genitori siano mai stati in prigione. Vengono altresì posti dei questionari volti a comprendere il pensiero dell'imputato come ad esempio: ''Si può essere aggressivi o pericolosi se qualcuno ci fa arrabbiare?''[274]. *COMPAS* si distingue da altri software di calcolo ''attuariale'', in quanto, oltre al fatto che tiene in considerazione sia i fattori di rischio dinamici che quelli statici, fornisce indicazioni non solo sul rischio di recidiva, ma anche su un trattamento individualizzato, basato sulla singola persona, per ridurre tale rischio[275].

Nonostante il grande e diffuso utilizzo dell'algoritmo *COMPAS* sono state sollevate alcune criticità in ordine alla sua effettiva validità predittiva (*accuracy*) e alla sua imparzialità (*fairness*). Da una ricerca effettuata da alcuni studiosi, nel maggio del 2016, è emerso che le previsioni formulate da *COMPAS* erano inaffidabili e risentivano di distorsione di tipo razziale,

[272]*Ibidem.*

[273]*Ibidem.*

[274]*Ibidem.*

[275]Cfr., Practitioner's Guide to COMPAS Core. Versione online del relativo "*Manuale operativo*", 2015.

considerato che su un campione di 7000 persone arrestate in Florida tra il 2013 e il 2014, veniva sovrastimato il rischio di recidiva in soggetti neri, rispetto a soggetti bianchi.[276]

Studi successivi[277] hanno sollevato ulteriori perplessità evidenziando che, oltre alle questioni relative al pregiudizio razziale, l'algoritmo *COMPAS* fornirebbe previsioni pressoché equivalenti a quelle fornite da persone prive di conoscenze specifiche in materia[278], dimostrando quindi una precisione scarsamente attendibile.

Altre critiche di maggiore gravità di *COMPAS* riguardano il suo possibile utilizzo in sede di *sentencing*, cioè a fini di commisurazione della pena dell'condannato. Tali critiche sono emerse in relazione al c.d. caso *Loomis*[279], dal nome di un imputato che aveva fatto ricorso alla Corte Suprema del Wisconsin per contestare l'entità della pena che gli era stata inflitta dalla Corte locale che, in fase commisurativa, si era avvalsa di *COMPAS*[280]: l'algoritmo predittivo veniva contestato per gli elementi pregiudizievoli basati sul genere e sulla razza presenti all'interno delle sue analisi, nonché per l'oscurità del meccanismo di funzionamento, che creava problemi di trasparenza.

---

[276]Cfr., ANGWIN J., KIRCHNER L., LARSON J., MATTU S., , *Machine Bias*, in *www.propublica.org*, 2016. In replica a tale studio, l'azienda produttrice di COMPAS ha commissionato una sorta di contro-studio, il quale avrebbe evidenziato una serie di errori nella metodica, nella misurazione e nella classificazione dei dati, commessi dai ricercatori di ProPublica: FLORES v. A., BECHTEL K., LOWENKAMP C., False Positives, False Negatives, and False Analyses: A Rejoinder to "*Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*", in *Federal Probation Journal*, 2016, (si noti, tuttavia, che tutti e tre gli Autori di questo contro-studio fanno parte del team di ricercatori di *COMPAS*). Per ulteriori riferimenti si può vedere direttamente la presente pagina del sito di *Equivant*.

[277]Cfr., DRESSEL J., FARID H., *The accuracy, fairness*, 3.

[278]Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 23.

[279]Cfr., Sul caso Loomis: ISTRIANI E., *Algorithmic Due Process: Mistaken Accountability and Attribution in State v. Loomis*, in *Harvard JOLT Digest*, 2017; FREEMAN K., *Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights* in *State v. Loomis, in North Carolina Journal of Law & Technology*, Vol. XVIII, 2016, 75 ss.; Anonimo, State v. Loomis. *Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing*, in *Harvard Law Review*, Vol. CXXX, 2017,1530 ss.; nella dottrina italiana, v. COSTANZI C., *La matematica del processo*, cit., 234; CARRER S., *Se l'amicus curiae è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin*, in *Giur. pen. web*,2019.

[280]Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 23.

La Corte Suprema del Wisconsin, sollecitata da tali rilievi, ha formulato un *warning* in relazione al futuro uso di *COMPAS*, mettendo in evidenza[281]: la sua natura di prodotto industriale, per cui protetto dal segreto sul funzionamento, il fatto che l'algoritmo tendeva a sovrastimare il rischio di commissione di reato a carico di alcune minoranze etniche, il fatto che le valutazioni di *COMPAS* nella prassi non erano individualizzate ma erano effettuate su base collettiva.

Nel caso di specie, la Corte, tuttavia, ha respinto il ricorso del sig. Loomis, sulla scorta della considerazione che le valutazioni di *COMPAS* non erano state "decisive", in quanto erano state pur sempre sottoposte al vaglio, al controllo, alla validazione di un giudice[282].

In conclusione, sulla validità della elaborazione dei *big data* e dell'utilizzo degli algoritmi predittivi, non si è concordi. Da un lato, c'è chi sostiene che il loro impiego renda le valutazioni di pericolosità criminale più affidabili e maggiormente esenti da pregiudizi e condizionamenti culturali e, chi, invece, solleva serie perplessità in ordine all'effettiva validità predittiva (*accuracy*) e all'imparzialità (*fairness*) di questi algoritmi, per i seguenti motivi[283]:

a) La possibilità di risultati scarsamente affidabili o comunque discriminatori.

b) Il difetto di trasparenza, dal momento che gli imputati, così come gli stessi giudici, in molti casi (ad esempio, nel caso di *COMPAS*) non hanno dettagli in ordine al funzionamento interno di questi *software*, che resta oscuro poiché tutte le informazioni sono coperte da segreto industriale, per cui si finisce per essere dipendenti da terzi.

c) La sussistenza di problemi etici e deontologici di deresponsabilizzazione dei giudicanti dal momento che la valutazione in ordine alla propensione dell'imputato a ripetere il delitto non trova più la soluzione in un criterio metodologico di accertamento del fatto ordinario e neppure nella

[281] *Ibidem.*

[282] *Ibidem.*

[283] Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 22.

puntuale prescrizione della legge, ma viene affidato a un algoritmo di valutazione del rischio, elaborato da un software giudiziario [...].[284]

Tutte queste considerazioni sembrano aver frenato ma non arrestato l'utilizzo in America dei modelli statistico-matematici di tipo predittivo, finalizzati alla valutazione della pericolosità sociale.

Diversa è, invece, la situazione in Europa dove gli algoritmi predittivi della pericolosità criminale, non hanno avuto ancora accesso alle aule penali. A precluderne l'accesso, vige l'art. 15 della direttiva 95/46/CE, confluito nell'art. 22 del nuovo Regolamento europeo in materia di protezione dei dati personali, entrato in vigore il 25 maggio 2018[285]. Tale articolo stabilisce, infatti, che: ''ogni persona ha il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità''[286]. Tuttavia, su tale articolo prevale l'art 11 della Direttiva 2016/680, che in quanto *lex specialis* prevale sul GDPR e che così recita: '' È pertanto opportuno per i settori in questione (si fa riferimento alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali) che una direttiva stabilisca le norme specifiche relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, nel rispetto della natura specifica di tali attività. Tali autorità competenti possono includere non solo autorità pubbliche quali le autorità giudiziarie, la polizia o altre autorità incaricate dell'applicazione della legge, ma anche qualsiasi altro organismo o

[284]Cfr., CANZIO, *Il dubbio e la legge,* in *Diritto penale contemporaneo,* 2018, 3 s. Sul classico ragionamento giudiziario "by probabilities", v. lo stesso CANZIO G., La motivazione della sentenza e la prova scientifica: "reasoning by probabilities", in CANZIO G.

[285]Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 24.

[286]*Ibidem.*

entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici ai fini della presente direttiva. Qualora tale organismo o entità trattino dati personali per finalità diverse da quelle della presente direttiva, si applica il regolamento (UE) 2016/679. Il regolamento (UE) 2016/679 si applica pertanto nei casi in cui un organismo o un'entità raccolgano dati personali per finalità diverse e procedano a un loro ulteriore trattamento per adempiere un obbligo legale cui sono soggetti. Ad esempio, a fini di indagine, accertamento o perseguimento di reati, gli istituti finanziari conservano determinati dati personali da essi trattati, e li trasmettono solo alle autorità nazionali competenti in casi specifici e conformemente al diritto dello Stato membro. Un organismo o un'entità che trattano dati personali per conto di tali autorità entro l'ambito di applicazione della presente direttiva dovrebbero essere vincolati da un contratto o altro atto giuridico e dalle disposizioni applicabili ai responsabili del trattamento a norma della presente direttiva; l'applicazione del regolamento (UE) 2016/679 rimane invece impregiudicata per le attività di trattamento svolte dal responsabile del trattamento di dati personali al di fuori dell'ambito di applicazione della presente direttiva''.

In ambito eurounitario, occorre ricordare che la Risoluzione del Parlamento europeo sulla robotica del 2017 pone come elemento essenziale il principio della trasparenza, sottolineando la necessità che risulti sempre possibile indicare la logica alla base di ogni decisione, avente impatto sulla vita di una o più persone, presa con l'ausilio dell'intelligenza artificiale[287].

Le perplessità legate all'uso degli algoritmi predittivi per la valutazione della pericolosità criminale sono state condivise, altresì, dalla Commissione per l'efficacia della giustizia (CEPEJ) del Consiglio d'Europa che ha elaborato la c.d. Carta etica. La Carta ribadisce che l'uso di algoritmi in materia penale al fine di mappare la personalità delle persone è stato criticato dalle ONG «a causa dei limiti della metodologia utilizzata[288]», e in particolare del loro «approccio meramente statistico[289]», il quale avrebbe «effetti discriminatori e

[287] *Ibidem.*

[288] *Ibidem.*

[289] *Ibidem.*

deterministici[290]», sicché esso andrebbe «sostituito da un altro approccio che risulti più rispettoso delle norme europee in materia di sanzioni penali e coerente con le *chances* di riabilitazione e reintegrazione del singolo individuo. Se i sistemi algoritmici riuscissero a migliorare, invece, la raccolta di informazioni per valutazioni inerenti alla *probation*, e a velocizzare la raccolta e il confronto di svariate informazioni con successivo controllo e verifica umani, allora ci sarebbe sicuramente di un progresso (specie nei procedimenti sommari) coerente anche con il principio di economia processuale. Qualsiasi altro uso è esposto al rischio di pregiudizi destinati ad entrare in conflitto con alcuni principi fondamentali, nazionali e sovranazionali»[291].

7.1 Strategie e tecniche dell'accusa basata su algoritmi: l'esperienza statunitense

Tradizionalmente l'attività del Pubblico Ministero è fondata su un lavoro di indagine che si basa, soprattutto, sull'analisi di documentazione cartacea presso Cancellerie e Uffici giudiziari. Lo stesso accade, nei dipartimenti di polizia dove abbondano fascicoli di ogni tipo. Si finisce, così, per trovarsi davanti la situazione di Uffici colmi di documenti pieni di informazioni complesse da esaminare, in un contesto di indagine ben organizzata ma frammentaria.

Le nuove tecnologie di analisi dati, basate su algoritmi predittivi, capaci di conoscere le correlazioni tra una vastissima quantità di informazioni, di difficile comprensione all'occhio umano, aiutano nella elaborazione di nuove strategie investigative, basate sui cosiddetti fattori di rischio.

Negli Stati Uniti, dove queste tecnologie sono già applicate, si sta assistendo all'ascesa della *intelligence-driven*, una nuova strategia di azione penale, centrata sui dati o, meglio, sulla elaborazione e condivisione dei *big data*, cambiando, così, le tattiche di accusa in molte giurisdizioni. Il primo

[290] *Ibidem.*

[291] Cfr., BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine, DPU-DIRITTO PENALE E UOMO*, (Fascicolo 10/2019), (2019), (pag.22-23-24). *Carta etica* pag 67 ss.

ufficio che si è affidato all'*intelligence-driven* è quello del procuratore distrettuale di Manhattan (ManhattanDA), sotto la *leadership* del procuratore distrettuale Cyrus Vance Jr.[292]. L'ufficio ha istituito la prima unità di strategie criminali, ''*The Crime Strategies Unit''* (CSU), nel 2014 volta a sviluppare un "*Intelligence-Model* di azione penale guidata." che individuasse sul territorio, le persone con la maggiore propensione a delinquere[293]. A Manhattan, per esempio, la CSU ha cercato una modalità volta adottare una indagine sui modelli di criminalità localizzati.[294]

L'intera Manhattan era stata divisa in cinque zone geografiche con una piccola squadra di procuratori assegnata a ciascuna area[295]. Successivamente, la CSU si è concentrata sull'individuazione del crimine a livello distrettuale. Il capo della CSU ha avviato un processo di raccolta di informazioni che ha coinvolto: mappatura dei modelli di criminalità, monitoraggio dei dati demografici e allocazione dei punti "caldi" all'internodi ventidue distretti di polizia, oltre che informazioni sulle varie bande criminali[296].Il risultato è stato quello di identificare un modello storico di atti violenti o criminalità reiterata legato alla zona geografica. Ciascuno dei ventidue distretti ha quindi generato un elenco di venticinque bersagli primari ("criminali prioritari" o c.d. '*'priority offenders*''), individui ritenuti i maggiori responsabili dell'attività criminale nel distretto.[297] Queste persone sono state quindi evidenziate dall'analisi per renderli inabili all'azione criminale attraverso procedimenti tattici-repressivi.[298] La teoria mirava a diminuire i modelli complessivi di criminalità, ponendo l'attenzione sui maggiori soggetti di rischio. La strategia, in parte guidata dai dati e in parte guidata dall'intelligenza umana, ha portato alla

[292]Cfr., FERGUSON Andrew G., *big data prosecution and brady UCLA law review*, vol. LXVII, 1, 2020, 189.

[293]Cfr., TALLON JENNIFER A. ET AL., *ctr. for court innovation, the intelligence- driven prosecution model: a case study in the new york county district attorney's office*, 2016, 5.

[294]Cfr., O'KEEFE David, *Head of the Manhattan District Attorney's Crime Strategies Unit*, in *CTR. FOR CT. INNOVATION*, 2013.

[295]Cfr., TALLON JENNIFER A. ET AL., *ctr. for court innovation, the intelligence- driven prosecution model: a case study in the new york county district attorney's office,* 2016, 8.

[296]*Ivi,* 13 ss.

[297]Cfr., FERGUSON Andrew G., *big data prosecution and brady UCLA law review*, vol. LXVII, 1, 2020, 190.

[298]*Ibidem.*

elaborazione di mappe digitali dettagliate sui crimini, fascicoli informatici di sospetti e a una migliore comprensione dei legami tra i luoghi, persone e modelli di attività illecita in aree localizzate.[299]

Oltre al *targeting* geografico e umano, il procuratore distrettuale di Manhattan ha organizzato trentatré *Bureau-Based Projects* (*BBP*) che si sono concentrati su particolari reati, ad esempio stupefacenti, furto aggravato, o su particolari bande in città[300]. Queste squadre *BBP* hanno coinvolto un piccolo gruppo di pubblici ministeri per specializzarsi nei particolari tipi di criminalità o gruppi in questione.[301] Ancora, come gli studi a livello di distretto, l'*intelligence* basata sui tipi di crimine ha consentito di prendere di mira le persone coinvolte in atti ripetitivi di particolare criminalità.

A San Francisco, il procuratore distrettuale George Gascón ha adottato un simile approccio accusatorio, basato sull'*intelligence* dell'accusa, l'ufficio del procuratore distrettuale di San Francisco in parte riorganizzato il sistema in un modello CSU[302]. Pur non essendo un programma così espansivo come quello realizzato a Manhattan, ha avuto lo stesso obiettivo di studiare i modelli di criminalità per colpire le aree a rischio più elevato e gli individui ad alto rischio di delinquenza.

Questi progetti tendono a concentrarsi sul rapporto tra persone, luoghi ed eventi criminosi. Da tali analisi si è riscontrato, ad esempio, che a San Francisco, solo 5 per cento dei delinquenti sono responsabili del 25 per cento dei reati. Solo l'uno per cento delle aree stradali risultava colpita da frequenti episodi di furti con scasso delle automobili, rendendolo uno dei maggiori problemi di criminalità a San Francesco. Quasi il 60% degli omicidi avviene con armi nei punti caldi della violenza.

Queste tecniche di persecuzione mirata di solito riguardano crimini violenti. In uno degli esempi più noti promossi di azioni penali guidate

[299]*Ibidem.*

[300]Cfr., FERGUSON Andrew G., *big data prosecution and brady UCLA law review,* vol. LXVII, 1, 2020, 180 e 256.

[301]*Ibidem.*

[302]Cfr., UCHIDA CRAIG D. ET AL., *A guide for implementing a crime strategies unit: the san francisco experience,* 2017, 3 e 6.

dall'intelligence, l'ufficio del procuratore distrettuale di Manhattan ha intentato una causa per cospirazione contro 103 imputati in due quartieri separati.[303]Queste azioni penali comportavano un'ampia sorveglianza di *social media*, comunicazioni e raccolta di intelligence.[304] Dopo mesi di indagini, la polizia ne ha arrestati decine, il metodo basato sull'*intelligence*, sebbene fosse focalizzato principalmente su reati gravi, ha anche scovato i crimini sulla qualità della vita come l'evasione delle tariffe di trasporto pubblico, i borseggi e la vendita di biglietti contraffatti[305]. Tale *targeting* spesso identifica, quindi, anche le persone che infrangono ripetutamente la legge con reati minori.

Nel corso di sei anni, 377 membri di bande sono stati incriminati attraverso questi metodi investigativi della CSU di New York. Sebbene principalmente focalizzato su reati gravi, il metodo basato sull'intelligence ha condotto l'accusa a un reato minore.

Oltre a catturare un quadro globale dell'attività criminale, con la conseguenza di una riduzione della delittuosità sul lungo termine, l'azione penale guidata dall'*intelligence* supporta anche una più ampia condivisione delle informazioni all'interno del sistema di giustizia penale.[306] Questo *focus* strategico ha permesso ai pubblici ministeri di vedere i collegamenti tra individui e gruppi e condividere più facilmente informazioni rilevanti su imputati, testimoni e vittime in giro per la città.

Tutto questo è stato reso possibile dai nuovi progressi tecnologici.

L'accusa guidata dall'*intelligence* ha iniziato a utilizzare nuovi dati basati supportati dalla tecnologia per rendere più agevole la raccolta e il riordino delle informazioni su comunità, crimini e presunti criminali. L'idea di base è caricare il *fileset* di dati centralizzato che possono essere cercati, mappati e collegati insieme per assistere i pubblici ministeri nel visualizzare le minacce e indagare

---

[303]Cfr., CAVALIERE Victoria, *More Than 100 Indicted in Harlem in Largest-Ever NYC Gang Bust*, in *REUTERS*, 2014), *https://www.reuters.com/article/us-usa-crime-gangs/more-than-100-indicted-in-harlem-in-largest-ever-nyc-gang-bust-idUSKBN0EF1DQ20140604.*

[304]Cfr., ID.;GOODMAN J. David, *Dozens of Gang Suspects Held in Raids in Manhattan*, in *N.Y. TIMES*, 2014, *https://www.nytimes.com/2014/06/05/nyregion/dozens-ofsuspected-gang-members-arrested-in-raid-of-2-harlem-housing-projects.html.*

.[305]Cfr., FERGUSON ANDREW G., *Big data prosecution and brady UCLA law review*, vol. LXVII, 1, 2020, 180 e 256.

[306]*Ivi,* 19 e 32.

sui crimini.[307] Grazie a queste tecnologie dei *big data*, i procuratori riescono a raccogliere, ordinare e collegare informazioni su atti e modelli criminali in una particolare area geografica, in modo più agevole.

Dette informazioni forniscono notizie in relazione ai casi attivi-aperti e chiusi; ai crimini dove non c'è un sospettato e quindi archiviati; ai dati relativi ai luoghi di attività criminale; ai dati relativi a soggetti potenzialmente più pericolosi; ai dati relativi a reti o bande criminali; dati relativi a persone in libertà vigilata o condizionale[308].

In particolare, la raccolta e l'analisi dei dati relativi ai casi attivi (*activecases*) ha eliminato i fascicoli scritti a mano con note, documenti, fotografie e quant'altro fosse associato a un caso e l'archiviazione cartacea è stata sostituita da equivalenti digitali. Le informazioni, che prima erano conservate in un archivio, ora sono registrate nel *server* di computer o presso *clouds* (*server* di archiviazione cui si accede tramite internet).

L'ufficio del procuratore distrettuale di Manhattan utilizza "*DANY Case Management*" per tenere traccia dei casi attivi nel sistema[309]. Tutte le informazioni vengono inserite in modo strutturato, in diversi campi (nome, sentenza, accuse, udienze, numeri di causa, ecc.) e possono essere facilmente reperite e confrontate. Sono, altresì, indicate le date delle udienze e altri dettagli importanti come informazioni sugli imputati, comprese le informazioni sull'ora e il luogo di arresto, quale distretto e agenti erano coinvolti, il tipo di accuse, i testimoni, l'affiliazione a bande, le chiamate ai servizi di emergenza e altri elementi chiave di un determinato caso giudiziario[310].

La digitalizzazione di tutte queste informazioni fornisce un *set* di dati centralizzato sui casi, consentendo di evidenziare su un determinato territorio, i tipi di crimine, i tassi di criminalità, luoghi, bande, ecc.[311]. Inoltre, queste

---

[307]Cfr., Cfr., UCHIDA CRAIG D. ET AL., *A guide for implementing a crime strategies unit: the san francisco experience,* 2017, 4.

[308]Cfr., FERGUSON ANDREW G., *Big data prosecution and brady UCLA law review*, vol. LXVII, 1, 2020, 180 e 256.

[309]*Ivi,* 39.

[310]*Ibidem.*

[311]Cfr., FERGUSON Andrew Guthrie, *Predictive Prosecution*, in *WAKE FOREST*, 2016, 720–721, 51, ("Intelligence-driven prosecution is not just about being smarter, but developing actionable

informazioni[312] possono aiutare i pubblici ministeri a conoscere un determinato territorio evidenziando la presenza di aree problematiche e/o di persone problematiche, riuscendo a identificare anche tutti i testimoni associati a delle circostanze di fatto[313].

La gestione dei dati sui reati non imputati aiuta alla individuazione di persone sospette in casi archiviati o nella situazione in cui sia stato compiuto un crimine in cui non vi sia ancora un sospettato[314]. L'analisi di questi dati è molto importante perché esaminando e comprendendo questi reati, si cerca di capire e, forse prevenire, crimini futuri sviluppando schemi relativi ad attività criminali non imputate, ma di assai probabile commissione[315].

L'ufficio del procuratore distrettuale di Manhattan, per aiutare la giustizia penale a prevenire la delinquenza, ha sviluppato il ''*Crime Prevention System*'' (*CPS*) ossia un "Sistema di prevenzione del crimine" che traccia i modelli di reato, imputati e non imputati, che si verificano in determinate zone al fine di catalogare e comprendere ogni evento criminale in un'area, indipendentemente dal fatto che vi sia o meno un procedimento giudiziario in corso. Con il *CPS*, i pubblici ministeri possono utilizzare il database per cercare determinate persone, bande, indagini o incidenti anche senza un'' caso attivo''[316].

Supponiamo, ad esempio, che un crimine grave si verifichi senza un'iniziale evidente sospetto; il database *CPS* registrerà il tipo di reato in un sistema di caselle di controllo: omicidio, colpi d'arma da fuoco, accoltellamento, furto in casa, rapina, furto con scasso commerciale, polizia

---

intelligence about crime patterns in an area. Finally, all of this information about past criminal activities is memorialized in a searchable dataset for future action.").

[312]Cfr., GANSLER Douglas F., *Implementing Community Prosecution in Montgomery County, Maryland*, in *PROSECUTOR*, 2000, at 30, 30–31.

[313]Cfr., HOLDER Eric, *Community Prosecution*, in *PROSECUTOR*, 2000, 31, 32 (discussing the importance of prosecutors knowing their community, the individuals involved in criminal activity, and seeing that crime is geographically based and sometimes connected).

[314]Cfr., FERGUSON Andrew G., *Big data prosecuton and Brady UCLA law review*, 2020, vol. LXVII, 1, 180 e 256.

[315]*Ibidem.*

[316]Cfr., TALLON JENNIFER A. ET AL., *Ctr. for court innovation, the intelligence- driven prosecution model: a case study in the New York county district attorney's office,* 2016, 5 *https://www.courtinnovation.org/sites/default/files/documents/IDPM_Research_Report_FINAL.PDF[https://perma.cc/25LC-JXST]* (evaluating the Manhattan District Attorney's Intelligence-Driven Prosecution model).

coinvolta, ecc. Oltre al reato, i dettagli catalogati includeranno altresì: la posizione, il nome della vittima, l'età, l'indirizzo e le coordinate geografiche (*geo coordinates*)[317]. Verrà, infine, inclusa una descrizione dell'incidente basata sull'iniziale indagine[318].

Per mostrare il funzionamento dell'algoritmo il procuratore distrettuale di Manhattan ha descritto il ''Caso Jefferson'', relativo ad una sparatoria: ''un ragazzo è stato colpito una volta all'inguine sinistro da uno sconosciuto di fronte al 2227 della Second Avenue. L'autore del reato è fuggito dal luogo in una direzione sconosciuta. Nessun dato balistico recuperato, nessuno ha assistito all'incidente''[319]. A questo punto nome della vittima, età, relazioni, bande e analisi dei possibili moventi possono essere inclusi nel *file system*[320].L'obiettivo è comprendere il contesto del reato. Per questo motivo tutti i dettagli utili sono inclusi nel *database CPS*. Ad esempio, il *software* contrassegna se sussistono dati correlati a violenza domestica, alla droga, alle bande o ai *club*; se sono presenti affiliazioni tra testimoni, imputati o vittime[321]. Il sistema potrebbe segnalare associazioni di bande, frequentazione di un particolare alloggio, edificio o quartiere[322], indicare se un reato potrebbe essere stato commesso come ritorsione tra bande rivali. Collegati al *CPS* sono, altresì, i dati relativi agli indagati e ai testimoni del delitto, informazioni personali incluso nome, data di nascita, soprannomi e le pagine*''Wiki''* (questi documenti vengono compilati ogni volta che un individuo viene contattato dalla polizia) oltre che dati raccolti dalla polizia[323]. Con il sistema digitale di gestione dei casi, i pubblici ministeri possono cercare in questi file digitali nomi, soprannomi, gang associazioni, o rivalità straordinarie, nuovi indizi possono emergere dai dati aggregati. Ad esempio, se un individuo è rimasto

[317]Cfr., FERGUSON Andrew G., *Big data prosecuton and Brady UCLA law review*, 2020, vol. LXVII 1, 180 e 256.

[318]*Ibidem.*

[319]Cfr., CHICON KERRY, *N.Y. county district att'y's off., intelligence-driven prosecution*:

[320]*Ibidem.*

[321]Cfr., FERGUSON Andrew G., *Big data prosecuton and Brady UCLA law review*, 2020, vol. LXVII 1, 180 e 256.

[322]*Ibidem.*

[323]*Ibidem.*

vittima di una aggressione nello stesso quartiere, anche senza testimoni dell'aggressione, la polizia potrebbe avere un indizio su un possibile motivo di ritorsione, o se ci fosse un omicidio la polizia potrebbe essere in grado di risalire a uno schema di violenza simile ed individuare più semplicemente il colpevole.

Questa raccolta di rapporti sugli incidenti del *CPS* dipinge un quadro del crimine locale ed individua *gang*, individui e faide che sono schedati e mappati. Anche senza arresti o sospetti, le forze dell'ordine possono comprendere meglio i crimini che si verificano in una zona e questo potrebbe essere utile per prevenire o risolvere crimini futuri, organizzando le forze dell'ordine in tal senso.

La tecnologia della mappatura è molto importante perché consente di individuare i luoghi in cui è più alto l'indice di criminalità e consente anche di conoscere e capire i quartieri più pericolosi e le aree o gli edifici dove la criminalità organizzata si riunisce (geografie delle bande), oltre a comprendere la rivalità tra bande attive da organizzare per tipo nel database CPS[324], nonché di identificare i luoghi di tutti gli arresti passati[325]e di visualizzare i crimini commessi nel passato[326].

Il fulcro dell'azione penale guidata dall'*intelligence* consiste, quindi, nell'identificare le persone ritenute responsabili di attività criminali in una determinata area,[327] con la convinzione che se ''i soggetti a rischio'' venissero rieducati, la criminalità sociale complessiva diminuirebbe[328]. Questo obiettivo coinvolge l'ausilio di quattro sistemi correlati: top 25, elenchi di bersagli, avvisi di arresto, *Wiki* e foto segnaletiche, che funzionano tutti insieme per informare i pubblici ministeri sulle persone con maggiore propensione al reato.

A Manhattan, i pubblici ministeri della CSU identificano circa 20-25 delinquenti in ogni distretto[329]. Questi soggetti sono di solito uomini che hanno

[324]*Ibidem.*
[325]*Ibidem.*
[326]*Ibidem.*
[327]*Ibidem.*
[328]*Ibidem.*
[329]*Ibidem.*

una storia di coinvolgimento criminale, incluse condanne penali[330], e sono inseriti nelle liste che indicano un'alta pericolosità, perché risultano coinvolti, spesso, in sparatorie o rapine, o perché soggetti a controllo o ad indagini della polizia[331]. Essere inseriti nella lista dei soggetti pericolosi comporterà che i pubblici ministeri potranno chiedere condizioni per il rilascio anticipato, prima del processo, più rigorose, potranno essere meno clementi nel patteggiamento o richiedere l'applicazione di pene più severe.[332]Inoltre, nei loro confronti, l'arresto diventa quasi un provvedimento automatico.

A Manhattan il sistema *Arrest Alert* (sistema di allarme arresto)compila una serie di informazioni di aiuto all'arringa accusatoria in tribunale.[333] Ad esempio, il sistema di allarme includerà: ''nome, *NYSID*, alias, affiliazione a bande, nonché altre informazioni sulle abitudini criminali passate (comprese etichette come ladri di biciclette, booster di auto); commissioni di crimini violenti; arresti per atti violenti commessi in stato di ubriachezza come un recidivo di dispositivo elettronico in libertà vigilata''[334]. Nello stesso sistema viene indicato se un imputato è stato segnalato dall'analisi del crimine *PBMN* (*Patrol Bureau of Manhattan North*) come un recidivo di dispositivo elettronico in libertà vigilata[335]o se vengono inserite nel database foto che ritraggono l'individuo in compagnia di soggetti armati di pistole.

Le informazioni che esistono in questo *database*, in continua espansione, sono condivise anche tra i pubblici ministeri che hanno bisogno di particolari indicazioni in tribunale[336]. L'innovazione del sistema di allerta di arresto, infatti, è quella di essere in grado di fornire ai pubblici ministeri le informazioni

---

[330]Cfr., Telephone Interview with O'KEEFE David & CHICON Kerry, *Crime Strategies Unit, Manhattan Dist. Attorney's Office*, 2016, (O'KEEFE David, one of the senior leaders of the Manhattan District Attorney's Crime Strategy Unit, stated that priority offenders usually had five or more felonies before being designated a priority target.).

[331]Cfr., FERGUSON Andrew G., *Big data prosecuton and Brady UCLA law review*, 2020, vol. LXVII 1, 180 e 256.

[332]*Ibidem.*

[333]*Ibidem.*

[334]*Ibidem.*

[335]*Ibidem.*

[336]Cfr., O'KEEFE David, *Head of the Manhattan District Attorney's Crime Strategies Unit*, in *CTR. FORCT. INNOVATION*, 2013).

necessarie per le determinazioni della cauzione nella prima fase del processo di giustizia penale[337], comprese le domande di cauzione prescritte. Queste informazioni frammentate possono essere condivise tra le giurisdizioni ed essere utili nel fornire il contesto di un sospetto arrestato in un altro caso. La teoria alla base di questa condivisione di informazioni è che, molte volte, i trasgressori prioritari vengono arrestati per reati minori ma magari sono responsabili di reati più gravi e rappresentano una grave minaccia per la comunità. Tali informazioni sono anche importanti perché possono determinare una cauzione più restrittiva e perché individuano i tipi di crimini che si verificano in determinati luoghi[338].

Questo tipo di informazioni personali su coinvolgimento criminale passato, amicizie, rivalità e simili non vengono segnalate solo nel sistema di allarme di arresto, ma vengono anche caricate su un sistema *Wiki*[339]. I sistemi *Wiki* si basano sull'approccio di *Wikipedia* alla condivisione delle informazioni in base al *crowd funding* di informazioni nella speranza che lo sforzo collettivo fornisca una descrizione più accurata di un argomento[340]. Nel contesto criminale, ciò significa che, tutte queste informazioni, comprese le note di *debriefing* dei detective e delle fotografie, vengono caricate sul sistema[341]. Se un procuratore vuole scoprire maggiori informazioni su un imputato o un testimone, deve solo cercare nel sistema.

Comprendere le reti di criminalità è una parte fondamentale dell'azione penale basata sull'*intelligence*[342].

Oltre a compilare informazioni su casi, crimini, luoghi e persone, i pubblici ministeri vogliono anche comprendere le relazioni associative e i collegamenti tra questi punti dati. La tecnologia consente ai pubblici ministeri di vedere

---

[337]Cfr., FERGUSON Andrew G., *Big data prosecuton and Brady UCLA law review*, 2020, vol. LXVII, 1, 203.

[338]*Ivi*, 205.

[339]Cfr., CHICON KERRY, *N.Y. county district att'y's off., intelligence-driven prosecution: Promoting collaboration*, 2010.

[340]Cfr., FERGUSON Andrew G., *Big data prosecuton and Brady UCLA law review*, 2020, vol. LXVII, 1, 205.

[341]*Ibidem.*

[342]Cfr., UCHIDA CRAIG D. ET AL., *A guide for implementing a crime strategies unit: the San Francisco experience*, 2017, 11.

queste connessioni anche tramite i social network, con l'ausilio di aziende private di analisi dati che offrono nuove capacità per cercare persone e connessioni[343]. Come spiega Elizabeth Joh, tale analisi dei *social network* delle forze dell'ordine può essere uno strumento investigativo molto potente: ''I *social network* si riferiscono a un insieme di connessioni personali tra un gruppo di persone. L'unità di base nell'analisi dei social network consiste nel legame tra due persone. I legami (rappresentanti le relazioni) tra i nodi (rappresentanti le persone) correlati da sistema possono assumere molte forme: transazioni, telefonate o contatti fisici tra vittime e trasgressori. Sulla base di una modellazione matematica, l'analisi dei social network mappa un particolare gruppo di relazioni''. Soprattutto, l'approccio identifica l'importanza relativa o la centralità dei nodi (individui): ''la loro importanza per il sistema criminale, il ruolo, il livello di attività, il controllo sul flusso di informazioni e le relazioni''[344].

Nel contesto della polizia, gli investigatori possono cercare nel set di dati arresti, proprietà, accuse e agenti di arresto e possono contrassegnare eventi, entità e documenti correlati. Gli investigatori possono utilizzare i filtri per cercare telefonate, e-mail, foto, incarichi di polizia, attività o comunicazioni di *Facebook*, e altro[345]. In definitiva, tutti questi punti dati e connessioni ricercabili consentono ai pubblici ministeri di collegare le persone con numeri di telefono comuni, indirizzi, voli condivisi o amicizie condivise[346].Ad esempio, la *tecnologia X1 Social Media*, mappa le connessioni scoperte[347], o *I2* una società che consente ai pubblici ministeri di condurre analisi dei collegamenti tra i numeri di telefono[348].

---

[343]Cfr., FERGUSON Andrew G., *Big data prosecuton and Brady UCLA law review,* 2020, vol. LXVII, 1, 206.

[344]Cfr., JOH Elizabeth E., *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, in *HARV. L. & POL'Y*, 2016, 15-25, 10, (quoting JOHNSON Jennifer A. et al., Social Network Analysis: A Systematic Approach for Investigating, in *FBI L. ENFORCEMENT BULL.*, 2013), http://leb.fbi.gov/2013/march/social-network-analysis-a-systematic-approach-for-investigating, *[http://perma.cc/47QG-ZNYC]).*

[345]Cfr., *Manhattan district att'y's office, models for innovation: the Manhattan district attorney's office 2010–2018*, 2018, 50 e 56.

[346]*Ibidem.*

[347]*Ivi,* 41 e 43.

[348]*Ibidem.*

I pubblici ministeri utilizzano, altresì, il sistema *DANY InPho* per tracciare le chiamate tra i detenuti delle carceri di New York City[349]. Il rapporto sulle chiamate dei detenuti NYC DOC consente ricerche per nome, numero, data, frequenza delle chiamate a determinati numeri[350]. Altre tecnologie permettono alla polizia di cercare e ordinare per indizi biometrici. *Photo Imaging Mugshot System* (PIMS) viene utilizzato a Manhattan per identificare i sospetti da una più ampia collezione di foto segnaletiche di arresto[351]. I pubblici ministeri possono confrontarsi con altri uffici per ricreare grafici di sospetti, collegare immagini come quartieri o bande, organizzare le indagini in base ai dati e anche con l'ausilio della tecnologia del riconoscimento facciale[352].Tutti questi diversi strumenti investigativi digitali forniscono un quadro migliore delle complesse relazioni tra diversi attori nel sistema di giustizia penale e sono ora disponibili per i pubblici ministeri con accesso al sistema[353].

Tradizionalmente, i pubblici ministeri sono al corrente di atti e questioni preliminari, processuali, di condanna e di appello, ma non sono altrettanto informati su imputati in libertà vigilata o condizionale. La nuova tecnologia sta cambiando questo focus, ampliando la rete di interessi e consentendo ai pubblici ministeri di rintracciare gli imputati rimessi in libertà vigilata[354] o rimessi in libertà dopo aver scontato la loro condanna[355] o anche suggerire condizioni di rilascio basate sul divieto di avvicinarsi a luoghi a rischio di criminalità.

8. Il *machine learning* e le sue potenzialità in campo penale

[349]*Ivi,* 52 s.

[350]*Ibidem.*

[351]*Ivi,* 22.

[352]*Ivi,* 51 e 56., si rimanda a GARVIE Clare, *Garbage In, Garbage Out: Face Recognition on Flawed Data,* in *GEO. CTR. ON PRIVACY & TECH.*, 2019.

[353]Cfr., FERGUSON Andrew G., *Big data prosecuton and Brady UCLA law review,* 2020, vol. LXVII, 1, 207.

[354]Cfr., TALLON JENNIFER A. ET AL., C*tr. for court innovation, the intelligence- driven prosecution model: a case study in the New York county district attorney's office,* 2016, 6.

[355]Cfr., *Manhattan district att'y's office, models for innovation: the Manhattan district attorney's office 2010–2018,* 2018, 19.

Per intelligenza artificiale si intende la capacità di una macchina computerizzata, tramite strumenti di programmazione avanzata, creata dall'uomo e capace di ragionare anche autonomamente, spesso con output indipendenti dall'input umano.

McCarthy, creatore dell'espressione ''*Artificial Intelligence''*, fondava i suoi studi sulla premessa per cui ''ogni forma di apprendimento potesse essere descritta in maniera così precisa, tramite l'elaborazione di appositi software, da consentire a una macchina di simularla''[356].

L'intelligenza artificiale, a sua volta, si divide in intelligenza artificiale forte, e intelligenza artificiale debole.

La prima indica la capacità delle macchine di creare valutazioni del tutto autonome, non vincolata al linguaggio di programmazione iniziale; quindi, strumenti che posseggono un vero e proprio ''stato cognitivo''[357].La seconda, invece, indica una mera imitazione dell'intelligenza umana, quindi dipendente dall'input di programmazione.

Il problema derivante dall'intelligenza artificiale, in particolare da quella forte, consisterebbe nella imprevedibilità dei comportamenti della macchina, capace di assumere ragionamenti e analisi proprie e della incapacità del programmatore di averne dominio[358].

Tuttavia, l'intelligenza artificiale aiuta gli esseri umani a svolgere attività per loro quasi impossibili, come la capacità di confrontare grandissimi set di dati in pochissimi secondi, e di trovare associazioni tra loro in tempi davvero limitati[359].

---

[356]Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale,* RICERCA SCIENTIFICA UNIVERSITÀ ROMA TRE *(*a cura di*),* Roma, 2020, 16.

[357]Cfr., KAPLANJ., *Intelligenza artificiale. Guida al futuro prossimo*, in LUISS UNIVERSITY PRESS, (a cura di) 2017, 74 ss. ; 10 CARTHY J. MC, MINSKY M.L., ROCHESTER N., SHANNON C.E., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 1955, disponibile in *www-formal.stanford.edu.* ; 11 KAPLAN J., *Intelligenza artificiale*, cit., 2017, 19. ; 12 TURING A.M., *Computing machinery and intelligence*, in Mind, 1950, 433.

[358]Cfr., KAPLAN J., *Intelligenza artificiale*, cit., 2017, 19.

[359]Cfr., TURING A.M., *Computing machinery and intelligence*, in Mind, 1950, 433.

Se macchine sono in grado di ragionare e, sono in grado di farlo anche nelle forme di supporto alle attività giuridiche e di prevenzione al crimine, è facile comprendere l'interesse della polizia predittiva al loro uso, affidandosi a sistemi di protezione di diritto ''più calcolabili'' e di repressione del crimine più efficace.

Le possibili intersezioni tra diritto penale e intelligenza artificiale mostrano un'ottica futura basata su sistemi di analisi dati, autonomi dal pensiero umano, capaci di supportare la polizia e la giustizia nelle indagini o nel processo o nella quantificazione della pena o nella rieducazione e a condurre ad una soppressione del crimine con maggiori tassi di successo. Si parla dei sistemi di *machine learning* e in particolare di *deep learning*[360].

Il termine "apprendimento automatico" può essere definito un algoritmo che consente ai computer di imparare a eseguire attività, identificare relazioni e discernere schemi senza la necessità degli esseri umani di fornire le istruzioni sottostanti. Gli algoritmi convenzionali operano eseguendo in sequenza un file pre-programmato contenente un insieme di regole per raggiungere un determinato risultato[361]. Gli algoritmi di *machine learning* sono un sottoinsieme della intelligenza artificiale (AI) il cui compito è insegnare ai computer ad acquisire informazioni dai dati e a migliorare con l'esperienza, anziché essere appositamente programmato per riuscirci; in altre parole, più dati vengono studiati, più la macchina apprende, diventando sempre più autonoma in tale processo analitico. Questi sistemi vengono, inoltre, dotati di un set di esempi da parte dell'utente e programmati per apprendere autonomamente i dati inseriti.

Questa potente idea risale almeno al 1950, ma è stato completamente realizzato solo negli ultimi anni, rivoluzionando molteplici domini della scienza e della tecnologia, con diverse varianti di *machine learning* che dominano, e in alcuni casi abilitano, molteplici applicazioni come motori di

[360]Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale,* RICERCA SCIENTIFICA UNIVERSITÀ ROMA TRE *(*a cura di*)* , Roma, 2020, 16.

[361]Cfr., FERGUSON Andrew L., *ACS Central Science Virtual Issue on Machine Learning,* in *ACS Cent. Sci. Publications*, Vol. IV (8), 2018, Washington, Stati Uniti, 938.

raccomandazione al dettaglio, rilevamento e riconoscimento facciale, traduzione linguistica, guida autonoma e assistita, filtro antispam e riconoscimento dei caratteri. Sono quindi macchine in grado di "imparare dall'esperienza" e, quindi, di migliorarsi autonomamente.

Una delle possibili forme di *machine learning* è rappresentata dal *deep learning*, in cui l'apprendimento automatico avviene mediante l'impiego di reti neurali artificiali, percorrendo fino in fondo la via dell'equiparazione tra il cervello umano e quello meccanico[362].

A fini meramente descrittivo-classificatori, si distingue tra: l'algoritmo delinquente, l'algoritmo inquirente e l'algoritmo consulente e/o giudicante.

Il c.d. "algoritmo delinquente" comprende, al suo interno, le questioni relative agli *''Artificial Intelligence-Supported Crimes''*[363] e, quindi, quei reati compiuti tramite il supporto dell'IA. Si pensi, ad esempio, alle diverse tipologie di reati "informatici", alle frodi finanziarie, al traffico di sostanze stupefacenti, o, ancora, agli incidenti cagionati da automobili con pilota automatico[364].

Il ricorso, purtroppo sempre più frequente, all'intelligenza artificiale "a fini criminali" cagiona nuove modalità di offesa con le quali il giudice e il legislatore sono chiamati a confrontarsi, per fronteggiare le "nuove" esigenze di tutela tramite interventi capaci di tenere sotto controllo le potenzialità di offesa dell'algoritmo criminale, non essendo sufficienti le tutele già presenti per i c.d. reati tradizionali. In alcuni casi si pone in particolare il problema della "responsabilità indiretta dell'uomo" intesa come responsabilità del programmatore dell'algoritmo[365]. Nei casi in cui, tuttavia, il ragionamento analitico della macchina risulta del tutto indipendente dall'input umano è ancora più difficile imputare la colpevolezza.

---

[363]Cfr., BORSARIR., *Intelligenza Artificiale e responsabilità penale: prime considerazioni*, in *www.medialaws.eu*, 2019, 2, 3; KING T., AGGARWAL M., TADDEO M., FLORIDI L., *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions,* in *Science and Engineering Ethics Ethics*, 2019, 1 ss.; BASILE F., *Intelligenza artificiale e diritto penale*, cit.,24 ss.

[364]*Ibidem.*

[365]Cfr., BORSARI R., *Intelligenza Artificiale e responsabilità penale: prime considerazioni*, in *www.medialaws.eu*, 2019, 2, 3.

L'algoritmo investigante e/o inquirente, invece, è impiegato come strumento di supporto all'attività del pubblico ministero e della polizia [366] ed è presente all'interno dei c.d. software di polizia predittiva, i quali: ''rielaborando un numero di dati superiore a quelli che sarebbe in grado di gestire un operatore umano, indirizzano nella individuazione delle zone calde (*hotspots*), intese come quelle in cui è elevato il rischio della commissione di reati, oppure supportano nella attività di *crime linking*, prevedendo la futura commissione di reati da parte di soggetti determinati o da determinare''[367]. Esistono anche programmi ad ausilio della polizia per la ricostruzione dei fatti, tramite indizi. Tra questi rientrano, per esempio: *STEVIE*, un *software* che ricostruisce un iter storico possibile sulla base dei dati sottoposti ad analisi[368], mentre il *software* ALIBI valuta il comportamento di un soggetto a fronte di un reato che gli viene contestato e prevede la probabilità della commissione di crimini futuri sulla base della tecnica del ''Feature Importance'' con cui identifica quali variabili o caratteristiche hanno maggiore influenza sulle previsioni di delittuosità[369].

Di matrice italiana è, invece, particolarmente noto ''*KEYCRIME*'', un programma sviluppato dal poliziotto Mario Venturi e attualmente in dotazione alla Questura di Milano[370]. I dati dimostrano che l'impiego di *KEYCRIME* non solo ha determinato una significativa diminuzione di certi reati (soprattutto rapine), ma avrebbe fornito, altresì, un aiuto significativo nella risoluzione di reati già commessi[371]. La peculiarità del software consiste nella sua capacità di processare dati che attengono anche al profilo comportamentale dell'autore,

---

[366]Cfr., BASILEF., *Intelligenza artificiale e diritto penale*, cit., 32-33. 22.

[367]Cfr., BASILEF., *Intelligenza artificiale e diritto penale*, cit., 10 ss.

[368]Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale*, in RICERCA SCIENTIFICA UNIVERSITÀ ROMA TRE *(*a cura di*)* , Roma, 2020, 22.

[369]Cfr.,Amplius NISSANE., *Digital Technologies and Artificial Intelligence's Present and Foreseeable Impact on Lawyering, Judging, Policing and Law Enforcement*, in *AI&Soc*., 2017, 450 ss.

[370]Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale*, in RICERCA SCIENTIFICA UNIVERSITÀ ROMA TRE *(*a cura di*)* , Roma, 2020, 22.

[371]Cfr., PELLICCIA R., *Polizia predittiva: il futuro della prevenzione criminale?*, in www.cyberlaws.it, 2019.

aumentando il grado di*''accuracy''*, o di ''*reliability''* dell'analisi, rispetto ad algoritmi analoghi, [372]; il *software* è anche utilizzato per prevedere la futura commissione di reati da parte di un determinato soggetto[373].

Da ultimo l'algoritmo consulente e/o giudicante è uno strumento utile sia a supporto del giudice, ma anche per rafforzare il diritto di difesa[374].Tramite l'algoritmo consulente è possibile organizzare banche dati sempre più elaborate, che non rappresentano un mero deposito statico di dati e informazioni ''grezze'', ma che sono in grado di guidare l'utente nella ricerca dei riferimenti normativi e giurisprudenziali rilevanti o, addirittura, di formulare "pareri"[375].

Un esempio può essere quello di *''ROSS INTELLIGENCE''*, la versione legale del più noto *Watson Debater* di IBM, già ribattezzato come "SIRI for the law"[376]. Si tratta di un sistema in grado di offrire consigli legali a partire da: una illustrazione del fatto esposta in "inglese comune", riferimenti giurisprudenziali e citazioni di dottrina, e, "imparando dalle passate interazioni'', ogni analisi offerta da ROSS ne accresce la precisione per il futuro[377]. In altre parole, il *software* più risponde alle richieste degli utenti più impara.

Gli algoritmi consulenti, quindi, specie quelli che sfruttano il *machine learning* o addirittura il *deep learning*, consentono di prevedere, con un grado di attendibilità sempre crescente, l'esito di un processo, si tratta della nuova

---

[372]Cfr., BASILE F., *Intelligenza artificiale e diritto penale*, cit., 10 ss.; NISSAN E., *Digital Technologies and Artificia lIntelligence's Present and Foreseeable Impact on Lawyering, Judging, Policing and Law Enforcement*, in *AI&Soc*., 2017, 450 ss., 31; PELLICCIA R., *Polizia predittiva: il futuro della prevenzione criminale*, in *www.cyberlaws.it*, 2019, 2.

[373]Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale,* RICERCA SCIENTIFICA UNIVERSITÀ ROMA TRE *(*a cura di*)* , Roma, 2020, 22.

[374]Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale,* RICERCA SCIENTIFICA UNIVERSITÀ ROMA TRE *(*a cura di*)* , Roma, 2020, 23, V. amplius: O'DONNEL R.M., *Challenging Racist Predictive Policing Algorithms under the Equal Protection Clause*, in *New York University Law Review*, 2019, 544 ss.

[375]*Ibidem.*

[376]Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale,* RICERCA SCIENTIFICA UNIVERSITÀ ROMA TRE *(*a cura di*)*, Roma, 2020, 24.

[377]*Ibidem.*

''giustizia predittiva''[378]. È stato sviluppato, da un gruppo di ricercatori, un algoritmo, celebre per il suo alto tasso di successo, che è in grado di "calcolare" gli esiti delle sentenze della Corte europea dei diritti dell'uomo con un grado di precisione del 79%[379]. I ricercatori precisano che mentre gli studi precedenti valorizzavano metadati capaci di influenzare i pareri dei giudici come la gravità del reato, posizioni politiche del giudice[380]. Il loro studio mira a prevedere la decisione di un determinato caso sulla unica base di informazioni di carattere testuale[381]. L'esito dello studio, inoltre, rivelerebbe la rilevanza del "fatto" (caso *de quo*) rispetto al "diritto"[382].

[378]*Ibidem.*

[379]CFR., ALETRAS N., TSARAPATSANIS D., PREOTIUC-PIETRO D., AND LAMPOS V., *Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective*, in *PeerJ Computer Science*, 2016, 1 ss.

[380]Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale,* in RICERCA SCIENTIFICA UNIVERSITÀ ROMA TRE *(*a cura di*)* , Roma, 2020, 25.

[381]Cfr., ALETRAS N., TSARAPATSANIS D., PREOTIUC-PIETRO D., AND LAMPOS V., *Predicting judicial decisions of the European Court of Human Rights*, 2.

[382]Cfr., ALETRAS N., TSARAPATSANIS D., PREOTIUC-PIETRO D., AND LAMPOS V, *Predicting judicial decisions of the European Court of Human Rights*, 11 ss.

CAPITOLO II

PREDICTIVE POLICING

1. Nozioni preliminari: cosa si intende per ‘’*predictive policing*”?

Il *‘’predictive policing’’* consiste nell’applicazione di avanzate tecniche computerizzate di analisi dati, volte a identificare i probabili soggetti a rischio di pericolosità criminale ovvero i luoghi in cui avvengono maggiormente attività di delinquenza.

La definizione di polizia predittiva, in chiave estensiva, indica qualsiasi approccio legato alla lotta alla criminalità, che includa un affidamento a tecnologie dell'informazione, quali, in particolare, analisi dati, mappatura della criminalità[1], uso degli algoritmi predittivi[2], volto a migliorare la soppressione di attività *contra legem*. In termini semplici, la polizia predittiva coinvolge modelli computerizzati che identificano i luoghi in cui è presente il ‘’rischio‘’ di commissione di futuri reati sulla base di analisi statistiche su crimini passati e altri dati[3] ricercati di volta in volta, sulla base dell’indagine *ad hoc* da effettuare. Ad esempio, vengono confrontati dati storici su un particolare tipo di crimine con il luogo e l'ora della consumazione o ancora arresti, chiamate di servizio e segnalazioni di incidenti.

Queste informazioni vengono ponderate in base ai tipi di reato (reati violenti, reati contro il patrimonio) e includono anche dati su particolari individui[4], attività di bande, modelli di traffico, fattori ambientali e altre

[1] Si rimanda al capitolo 1, blue data.
[2]Cfr., PEARSALL Beth, *Predictive Policing: The Future of Law Enforcement*?, in N*at'l Inst. Just. J*., 2010, 16, ("Predictive policing, in essence, is taking data from disparate sources, analyzing them and then using results to anticipate, prevent and respond more effectively to future crime."), FERGUSON Andrew Guthrie, *Predictive Policing and Reasonable Suspicion*, (a cura di), 2012 in *Emory Law Journal*, vol. LXII, 2012, 259, 265.
[3]Cfr., FERGUSON Andrew Guthrie, *Predictive Policing and Reasonable Suspicion*, 2012 in *Emory Law Journal*, vol. LXII, 2012, 259, 265.
[4]Cfr., CASADY Tom, *Police Legitimacy and Predictive Policing*, in *Geography & Pub. Safety*, 2011, 1.

informazioni locali[5].Per cui il meccanismo di indagine della polizia predittiva si basa su algoritmi che analizzano i dati, cercando modelli di criminalità in particolare aree, statisticamente con propensione alla delinquenza più probabile[6]. Tramite appositi *software* predittivi, la polizia può migliorare la sua attività di repressione al crimine. In particolare, le forze dell'ordine, con l'ausilio di tali algoritmi, potrebbero sviluppare nuove strategie preventive, come un maggiore controllo di determinati luoghi o una migliore gestione delle risorse volta a minimizzare il rischio di criminalità. Mediante alcuni programmi avanzati, addirittura, tramite la tecnologia del *''real-time''*, la polizia potrebbe avere sotto controllo costante molte aree cittadine nelle operazioni di pattugliamento.

Questi strumenti, oggi molto utilizzati soprattutto negli Stati Uniti, aumentano notevolmente la dipendenza dei dipartimenti di polizia dalla tecnologia dell'informazione (*Information Technology—IT*) per raccogliere, mantenere e analizzare tali set di dati[7].

Le agenzie di polizia utilizzano, infatti, l'analisi computerizzata delle informazioni sui crimini passati, l'ambiente locale e altre informazioni pertinenti per ''prevedere'' e prevenire il crimine. L'idea è di migliorare la consapevolezza situazionale a livello tattico e strategico e di sviluppare strategie che promuovano attività di polizia più efficienti ed efficaci. Mediante la consapevolezza della situazione e l'anticipazione del comportamento umano, la polizia può identificare e sviluppare strategie per prevenire l'attività criminale da parte di recidivi contro vittime recidive. Questi metodi consentono inoltre ai dipartimenti di polizia di lavorare in modo più proattivo con l'ausilio di un minor uso delle risorse. Si mira, quindi, a produrre risultati tangibili come una diminuzione dei tassi di criminalità, un aumento dei tassi di arresto per

[5]Cfr., JIE XU ET AL., RUTGERS CTR. ON PUB. SEC., C*rime generators for shootings in urban areas: a test using conditional locational interdependence as an extension of risk terrain modeling*, 2010, 1.
[6]Cfr., PAUL Jeffrey S. & JOINER Thomas M., *Integration of Centralized Intelligence with Geographic Information Systems: A Countywide Initiative,* in *Geography & Pub. Safety*, 2011, 5 e 7.
[7]Cfr., PERRY Walter L., MCINNIS Brian, PRICE Carter C., SMITH Susan C., HOLLYWOOD John S., P*redictive policing, The Role of Crime Forecasting in Law Enforcement Operations*, in *Rand Corporation*, Santa Monica, 2013, 2.

reati gravi e un impatto positivo complessivo sia dal punto di vista sociale che quello giudiziario[8].

Il dipartimento di polizia di Los Angeles (LAPD), ad esempio, ha intrapreso un ambizioso progetto pilota per testare l'efficacia della polizia predittiva[9]. La polizia, sotto la guida dell'ex capo della polizia William Bratton, e con la collaborazione di studiosi di diverse università della California, ha avviato un piano incentrato sulla prevenzione di determinati crimini in determinate aree[10].Il progetto è stato sviluppato dal capitano della polizia di Los Angeles Sean Malinowski con il supporto degli algoritmi creati dal professor Jeffrey Brantingham dell'UCLA e dal professor George Mohler dell'Università di Santa Cruz. Il programma si concentra su tre specifici tipi di reati contro il patrimonio: furto con scasso, furto di automobili e furto da automobili[11] e sulla base di tre anni di dati, ponderando i reati più recenti rispetto a quelli più vecchi e osservando i modelli, l'algoritmo cerca di identificare aree di probabile attività criminale[12] indirizzando gli ufficiali dove è previsto il reato. I primi risultati hanno avuto successo, poiché la criminalità, relativamente ai reati sopra citati, è diminuita in quelle aree, sono tuttavia in corso nuovi esperimenti per testare l'affidabilità dell'algoritmo[13].

Un esperimento simile è quello fatto a Santa Cruz, in California, sulla base della ricerca condotta dal professor George Mohler. A Santa Cruz gli agenti hanno ricevuto quotidianamente "previsioni del crimine" della giornata, che li

---

[8]Cfr., PERRY Walter L., MCINNIS Brian, PRICE Carter C., SMITH Susan C., HOLLYWOOD John S., P*redictive policing, The Role of Crime Forecasting in Law Enforcement Operations*, in *Rand Corporation*, Santa Monica, 2013, 1 s.

[9]Cfr., FERGUSON Andrew Guthrie, *Predictive Policing and Reasonable Suspicion*, 2012 in *Emory Law Journal*, vol. LXII, 2012, 259, 267.

[10]*Ibidem.*

[11]*Ibidem.*

[12]*Ibidem.*

[13]Cfr., ADAMS Guy, *The Sci-Fi Solution to Real Crime*, in *Independent*, Londra, 2012, 32; RUBIN Joel, *Stopping Crime Before It Starts*, in *L.A. TIMES*, 2010, 1; CHRISTOPHER BEAM, *Time Cops: Can Police Really Predict Crime Before It Happens?*, in *Slate*, 2011, *http://www. slate.com/articles/news_and_politicscimet2Ol 1/01/time cops.single.html*; *Weekend Edition Saturday*, in *National Public Radio broadcast*, 2011, http://www.npr.org/2011/11/26/142758000/at-lapd-predicting-crimes-before-they-happen (*predictive policing* a Los Angeles; v. anche FERGUSON Andrew Guthrie, "*Predictive Policing" and the Fourth Amendment*, in *Am. Crim.*, 2011, *http://www.americancriminallawreview.com/Drupal/blogs/blog-entry/"predictive-policing"-and-fourth- amendment*-11-28-2011.

indirizzava a pattugliare determinate aree designate come più rischiose[14]. Ogni previsione prevedeva una percentuale di pericolo, ad esempio, la probabilità del 10,36% di furto d'auto [15] in un determinato garage al centro della città in un particolare momento del giorno[16]. Gli agenti di polizia venivano quindi inviati a pattugliare quelle aree come parte dei loro controlli regolari[17].Nei primi sei mesi dell'esperimento tredici persone sono state fermate nei luoghi designati come rischiosi[18].

I dipartimenti di polizia di Los Angeles e Santa Cruz, tramite queste nuove tecnologie di prevenzione, potrebbero essere in vantaggio rispetto ad altre città nel testare il modello di polizia predittiva. Altre giurisdizioni, sulla loro scorta, come Palm Beach County, Florida[19]; Memphis, Tennessee[20]; Chicago, Illinois[21]; Minneapolis, Minnesota[22]; e Dallas, Texas[23], stanno testando nuove tattiche di polizia predittiva per combattere reati di diversa entità mediante finanziamenti governativi. L'attenzione alla prevenzione è conveniente e utile perché favorisce la diminuzione dei costi comunali e statali[24], offre la promessa di un piano *high-tech* e progressista per fermare il crimine[25], e infine perché,

---

[14]Cfr., STUART Tessa, *The Policemen's Secret Crystal Ball*, in S*antacruz Wkly*., 2012, 9.
[15]*Ibidem.*
[16]Cfr., BAXTER Stephen, *Modest Gains in First Six Months of Santa Cruz's Predictive Police Program*, in S*antacruz Sentinel.*
[17]Cfr., STUART Tessa, *The Policemen's Secret Crystal Ball*, in S*antacruz Wkly*., 2012, 13 s.
[18]Cfr., BAXTER Stephen, *Modest Gains in First Six Months of Santa Cruz's Predictive Police Program*, in S*antacruz Sentinel*, 38 e 50.
[19]Cfr., BURDI Jerome, *Police Looking to Predict Crimes in Palm Beach County*, in *Palm Beach Sun Sentinel*, 2011, *http://articles.sun-sentinel.com/2011-10-30/news/fl-predictive-policing-20111030_1_violent- crime-police-stake-police-agencies.*
[20]Cfr., ASHBY Andrew, *Operation Blue CR.U.S.H. Advances at Mpd*, in *Memphis daily NEWS*, 2006, *http://www.memphisdailynews.com/editorial/Article.aspx?id=30029*, C.R.U.S.H. (Crime Reduction Using Statistical History) (diretto da).
[21]Cfr., News Briefs: *Chicago Police Department Adopts Predictive Crime-Fighting Model*, in *Geography & Pub.Safety*, 2011, 14.
[22]Cfr., MCKINNEY Matt, *The Next Crime*, in *Star Trib*., Minneapolis, 2011, 1, (*predictive policing units in Minneapolis*).
[23]Cfr., KENNEDY Leslie W. et al., *Risk Clusters, Hotspots, and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies*, in *Quantitative Criminology*, 2011, 339, 345-46, 27, e GASSAWAY Brigitte et al., *Engaging the Community: Operation Heat Wave*, in *Geography & Pub.Safety*, 2011, 8 s.
[24]Cfr., BECK Charlie & MCCUE Colleen, *Predictive Policing: What Can We Learnfrom Wal-Mart and Amazon About Fighting Crime in a Recession?*, in *Police Chief*, 2009, 18.
[25]Cfr., SKLANSKY David Alan, *the persistent pull of police professionalism* , 2011, 8 s., available at *http://www.hks.harvard.edu/var/ezpsite/storage/fckeditor/file/pdfs/centers-programs/programscriminal-justice/ExecSessionPolicing/NPIP-ThePersistentPullofPoliceProfessionalism-03-1l1.pdf*, 9.

dai primi test, seppur in aree piccole, la strategia, basata sul *data-driven*, sembra ridurre o quantomeno limitare la criminalità mediante un'attività ben organizzata della polizia.

1.1 Dal sospetto al crimine

Il *data mining cell-tower*, i metadati o i dati sul crimine si basano tutti sullo stesso principio: ossia sull'alta probabilità che le associazioni fatte dagli algoritmi riescono a collegare un sospetto, di difficile valutazione esclusivamente umana, a un crimine. Le probabilità, spesso statistiche, quindi suggeriscono i rischi di delinquenza con un alto grado di certezza.

Ma la questione è: ''Un algoritmo può essere sufficiente a fondare un probabile motivo di arresto?[26] Può un algoritmo ben programmato, privo di pregiudizi, con un alto livello di accuratezza, creare i presupposti per dimostrare la colpevolezza di un soggetto, anche tenendo conto degli elementi psicologici? Queste domande fondano la nuova questione del c.d. *data-driven policing puzzle*[27].

Due intuizioni contraddittorie, infatti, si scontrano quando si pensa alla pura probabilità. La prima consiste nel riconoscere che le previsioni, per definizione, possono essere sbagliate. La seconda riguarda l'incertezza del sospetto generato dall'apprendimento automatico. La mera correlazione di dati ''rischiosi'' o la probabilità matematica non sono sempre sufficienti per giustificare l'efficacia dell'azione della polizia.

Tuttavia, è necessario precisare, preliminarmente, che il sospetto predittivo non è un concetto completamente nuovo, essendo necessario per l'inizio di ogni indagine in capo a qualsiasi soggetto avente particolari caratteristiche coerenti con gli indizi del caso. Quando, ad esempio la polizia giudiziaria agisce per conto di un mandato di perquisizione del giudice, di fatti sta intervenendo in vista di una previsione circa il rischio o il sospetto che l'attività criminale sia

[26]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 124 s.
[27]*Ibidem.*

situata in quel particolare luogo oggetto di controllo[28]. Il giudice, che dispone il mandato, deve, a sua volta, prima determinare, esaminando i documenti, se c'è una adeguata probabilità che il crimine o le prove di un crimine si trovino in un luogo particolare[29]. È sempre possibile, però, che il giudice si sbagli. È possibile affermare, quindi, che sospetto predittivo deriva da quella che potrebbe essere definita la ‘‘*probable cause*’’[30].

Come ha dichiarato la Corte Suprema degli Stati Uniti: "Nel tipico caso in cui la polizia chiede il permesso di perquisire un'abitazione o un luogo al fine di rinvenire un determinato elemento probatorio o un oggetto rilevante per il caso, lo fa con la convinzione che si trovi lì, e la determinazione del magistrato, a sua volta, deriva dalla valutazione circa una *probable cause*, quindi la previsione, che l'oggetto sarà ancora lì quando il mandato sarà eseguito"[31].

La *probable cause*, come suggerisce il termine, quindi, è connessa alla rilevante probabilità. L'elemento focale è legato al fatto che la possibilità che un sospetto probatorio conduca o meno alla individuazione di un eventuale indagato o inchiodi la sua colpevolezza, non può mai essere quantificata al 100%.

Per questo la Corte Suprema, chiarendo la questione, si è rifiutata di fornire percentuali precise per definire quando una *probable cause* è pressoché certa[32].

Seppur nel nostro sistema la prova richiesta, tale da definire la completa punibilità di un individuo, sia ‘’al di là di ogni ragionevole dubbio’’, qui si tratta di definire una probabilità investigativa, tale da fondare meramente un sospetto, non una completa accusa.

La Corte Suprema ha dichiarato: "La causa probabile non è quantificabile con precisione in percentuali perché si tratta di probabilità dipendenti dalla totalità delle circostanze che quindi variano caso per caso"[33]. La ragione di

[28]Si veda, United States v. Grubbs, 547 U.S. 90, 95, 2006.
[29]Si veda, Illinois v. Gates, 462 U.S. 213, 238, 1983.
[30]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 124 s.
[31]V., Grubbs, 547 U.S., 95.
[32]Cfr., GOLDBERG Erica, *Getting Beyond Intuition in the Probable Cause Inquiry*, in *Lewis & Clarkl*, 2013, 789, 790-91, 17.
[33]Si veda, *Maryland* v. Pringle, 540 U.S. 366, 371, 2003.

questa mancanza di precisione è in gran parte dovuta al fatto che i giudici sono tenuti, in questa fase, a prendere decisioni rapide con informazioni imperfetta, legate al mero sospetto o persino ‘’rischio’’ di pericolosità, non ad una vera e propria accusa[34].

Un noto caso del 1968 (Terry contro Ohio) ribadisce il grado di certezza necessario delle motivazioni probatorie alla base di un arresto; la polizia deve, infatti, ‘’essere in grado di indicare fatti specifici e articolabili che, insieme alle inferenze razionali da tali fatti, giustificano ragionevolmente quell'intrusione nella sfera personale degli individui’’[35]. In altre parole, la polizia deve articolare il motivo alla base della predizione di criminalità in capo ad una certa persona. Ancora una volta, si ribadisce il concetto che la previsione può essere sbagliata, ma contiene comunque un preliminare giudizio predittivo e probabilistico.

Le previsioni sussistono, quindi, principalmente alla base delle indagini forensi. Ad esempio, una corrispondenza del DNA è, in realtà, una probabilità che i due campioni biologici corrispondano[36].La previsione può avere più o meno probabilità di errore (ad esempio per la rilevazione del DNA ci si avvale di appositi macchinari che difficilmente incorrono in errori, ma è possibile anche questo), ma resta comunque una previsione.

Esaminando il quadro probatorio in tal senso è facile dedurre che le nuove tecnologie predittive non sono così tanto diverse dalle semplici previsioni legate agli indizi che possono incorrere in errori esattamente come l’apprendimento automatico degli algoritmi. In quest’ottica la questione del sospetto predittivo e l’affidabilità o meno dei processi conoscitivi delle macchine non è poi così controversa; infatti, deve sempre esserci una base probatoria che attesti la eventuale colpevolezza dell’imputato[37]. I veri problemi nascono quando invece si utilizzano tali algoritmi per prevenire totalmente il

[34] V., 6. *Gates*, 462 U.S., 231.
[35] Si veda, Terry v. Ohio, 392 U.S. 1, 21-22, 1968.
[36]Cfr., KAYE David H., *Rounding Up the Usual Suspects: A Legal and Logical Analysis of DNA Trawling Cases*, in *N.C.* 2009, 425-439, 87; ROTH Andrea, *Safety in Numbers? Deciding When DNA Alone Is Enough to Con-vict*, in *N. Y.U.*, 2010, 1130-1134, 85.
[37]Cfr., LOW Arnold H., *Rethinking Search and Seizure in a Post-911 World*, in *MISS.*, 2011, 1507-1518, 80.

crimine e quindi tracciare un profilo di alcuni soggetti potenzialmente pericolosi che nella prassi potrebbero non esserlo. Si tratta delle valutazioni sui luoghi ad ''alta criminalità'' o sulle *''heat people''*[38]o su un determinato ambiente considerato pericoloso. In quest'ambito, infatti, l'erronea valutazione di un soggetto potrebbe inficiare un'intera analisi algoritmica. Sostanzialmente il solo *data mining* probabilistico potrebbe essere insufficiente a definire la temibilità di alcuni soggetti, essendo necessario affiancare, alle valutazioni algoritmiche, taluni elementi che presentano maggiore certezza e rilevanza, al punto da definire una concreta volontà di delinquere.

Ma questo requisito risulta di difficile applicazione. Il punto focale è che anche se l'algoritmo o il sistema di allarme possono aiutare a trovare l'ago nel mio pagliaio, un essere umano dovrebbe confermare che la correlazione ha una concreta rilevanza investigativa nel caso particolare.

Daniel Steinbock ha sostenuto: "La profilazione predittiva non è incompatibile con il Quarto Emendamento, ma i fattori utilizzati per l'analisi algoritmica devono indicare agli agenti investigativi il grado di precisione del sospetto richiesto[39]. Tecnologia dei big data, nel futuro, quindi, se resa sempre più precisa, potrebbe bastare alle attività di *law enforcement''*. Tuttavia, attualmente, la questione sull'ammissibilità o meno, nei procedimenti, del puro sospetto algoritmico resta aperta.

Un'altra questione problematica è quella della affidabilità del c.d. ''sospetto individualizzato'' creato da un algoritmo. Bernard Harcourt e Tracey Meares spiegano le difficoltà di questo tema: ''Il sospetto configura alcuni gruppi di soggetti ''rischiosi'' e analizza la corrispondenza dei loro tratti a quelli di un individuo sottoposto ad analisi, come ad esempio l'abbigliamento, un determinato *modus* di descrizione degli eventi, quindi un'affinità colloquiale con i soggetti c.d. ''pericolosi'', determinati atteggiamenti o attitudini ... Si tratta di determinazioni, basata sui comportamenti di un

[38]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 126.
[39]Cfr., HARCOURT Bernard E. & MEARES Tracey L., *Randomization and the Fourth Amendment*, in *U. CHI.*, 2011, 809-813, 78.

individuo, spesso fatte indipendentemente dalla effettiva appartenenza al contesto criminale, che, però, se coincidono indicano un potenziale legame con il gruppo. Il sospetto in questi casi si definisce "individualizzato", ma, di fatto, si traduce nell'attacco ad un determinato un individuo solo perché confrontato con comportamenti del gruppo sospetto. In altre parole, nella maggior parte dei casi di polizia, il sospetto non ha origine a livello individuale[40] e, de facto, tende alla banale generalizzazione dell'azione del singolo come quella di gruppo. La polizia usa spesso queste scorciatoie cognitive, anche se spesso risultano pregiudizievoli, esplicitamente o implicitamente, e imprecise, inficiando, così anche l'apprendimento algoritmico. Il problema resta e si spera in una risoluzione futura, mediante *data mining* più efficaci e meno generalizzati.

2. L'influenza degli aspetti antropologici

In un ufficio accademico nel campus dell'Università della California-Los Angeles (UCLA), il già citato[41] professor Jeff Brantingham studia i c.d. *''hunter-gatherers''*[42] (i criminali) usando modelli computerizzati. L'antropologo ha scritto numerosi articoli su una varietà di argomenti, tra cui si ricordano titoli come "*Speculation on the Timing and Nature of Late Pleistocene Hunter-Gatherer Colonization of the Tibetan Plateau''* e "*Non linear Dynamics of Crime and Violence it Urban Settings*"[43]. Tutti i suoi lavori posseggono un importante filo conduttore nonché uno scopo: la capacità di mappare modelli dinamici predittivi dell'azione umana tramite modelli matematici, quindi volti alla prevenzione del crimine. I criminali vengono quindi paragonati a diversi tipi di *''hunters''* che, diversamente dai predatori animali, cacciano vittime[44].

---

[40]Cfr., STEINBOCK Daniel J., *Data Matching, Data Mining, and Due Process*, in *GA.*, 2005, 1-30, 40.

[41]V. paragrafo 1.

[42]*Cfr.*, FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 64.

[43]V., le pubblicazioni di BRANTINGHAM Jeffrey elencate in questo sito web universitario, *http:// paleo.sscnet.ucla.edu.*

[44]Cfr., HOFF Sam, *Professor Helps Develop Predictive Policing by Using Trends to Predict, Prevent Crimes*, in *Daily Bruin*, 2013, *http://dailybruin.com.*

Brantingham, sulla base delle sue ricerche, prendendo spunto anche da quelle dei genitori, due rinomati criminologi ambientali, è riuscito a dedurre l'intuizione che gli ambienti amplificano il rischio criminale creando un *software ad hoc* e costituendo un'impresa commerciale poi diventata multimilionaria. Il *software* prende il nome di PredPol (abbreviazione di "*predictive policing*"[45]) e nel tempo è diventato il leader nella tecnologia di polizia predittiva degli Stati Uniti basata sul luogo[46].

L'algoritmo posto alla base della programmazione di Predpol è stato creato sullo spunto di un precedente algoritmo, originariamente utilizzato e sviluppato per misurare le scosse di assestamento sismiche dai terremoti. Il motivo di questa somiglianza è semplice; i ricercatori hanno scoperto che così come da una scossa ne deriva un'altra e un'altra ancora, da un crimine, a catena, se ne scatenano tanti altri di medesima entità e negli stessi luoghi[47]. Quindi, così come le piccole crepe del terreno potrebbero anticipare una scossa sismica forte, alcuni elementi potenzialmente lesivi una volta identificati, potrebbero prevedere e mappare il crimine futuro.

L'intuizione che certi crimini abbiano qualità contagiose, tuttavia, non è una novità e, di fatto, ha un profondo sostegno nella teoria della criminologia[48].

Alcuni studi hanno, infatti, ripetutamente dimostrato la natura ''contagiosa'' dei crimini, osservando che alcuni comportamenti illeciti associati ad un determinato luogo come il furto con scasso incoraggiano altri soggetti tendenzialmente pericolosi a fare lo stesso, sull'idea che quel luogo sia ''sicuro'' in quanto poco controllato o nella generalità dei casi o particolarmente isolato[49].

---

[45]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 65.

[46]Cfr., BAILEY Ronald, *Stopping Crime before It Starts*, in *Reason*, 2012, *http:// reason.com*.; GORDON Leslie A., *Predictive Policing May Help Bag Burglars- but It May Also Be a Constitutional Problem*, in *A.B.A.J.*, 2013, *www.abajournal.com*.

[47]Cfr., RUBIN Joe, *Stopping Crime before It Starts*, in *L.A.Times*, 2010.

[48]*Ibidem.*

[49]Cfr., CHAINEY Spencer, TOMPSON Lisa, & UHLIG Sebastian, *The Utility of Hotspor Mapping for Predicting Spatial Patterns of Crime*, in *Security J.*, 21 4, 5.
(2008) BRAGA Anthony A., HUREAU David M., & PAPACHRISTOS Andrew V., *The Relevance of Micro Places to Citywide Robbery Trends: A Longitudinal Analysis of Robbery Incidents at Street Corners and Block Faces in Boston*, in *J. Res. Crime & Delinq.*, 2011, 48, 7 e 9.

Il professor Kent Kiehl, importante studioso di neurobiologia e neurocriminologia, autore di ‘’The Psycopath Whisperer’’, si è occupato, altresì, di analizzare il comportamento criminale, con l’ausilio di numerose risonanze magnetiche fatte ad alcuni condannati per reati gravi nelle carceri degli USA. Dalla ricerca è emerso che la maggior parte delle risonanze mostravano un’attività compromessa nella zona del cervello del sistema limbico, responsabile della gestione e del controllo delle emozioni. Il prof. Kiehl ha voluto sottolineare la possibile funzione preventiva derivante da tale analisi, in quanto curando e allenando la zona del cervello ‘’poco allenata’’ è possibile recuperare la funzione ad essa associata, soprattutto nei soggetti in giovane età[50].

Sulla base di quanto espresso, i criminali risultano essere creature abitudinarie e tendono a continuare a svolgere le loro operazioni illecite laddove ci sono pochi controlli delle forze dell’ordine, e meno possibilità di essere catturati.

Si è cercato di dare anche una spiegazione al fenomeno per cui i criminali tendono a tornare nel luogo sul delitto anche dopo la commissione del fatto.

Come ha spiegato Shane Johnson, "Dopo aver preso di mira una determinata abitazione, per la prima volta, un ladro acquisisce conoscenze per determinare le future decisioni sul come agire. Questo può riguardare lo studio degli interni di una proprietà, la percentuale di difficoltà per lo scasso, la facilità di accesso e fuga, le prove che potrebbero inchiodarlo se il medesimo autore del reato deve tornare sul luogo del delitto, i rischi di identificazione e così via. È probabile che questa conoscenza riduca l'incertezza, per il reo, delle informazioni delle case vicine’’[51].

Nel corso degli anni, i criminologi hanno cercato di studiare il c.d. *‘’near repeat’’*, cioè quel fenomeno per cui i criminali tendono a ripetere i delitti in un medesimo luogo o in uno molto vicino a quello precedente (es. una casa

[50]V., *https://traileoni.it/2021/03/neurocriminologia-linfluenza-dei-geni-sul-comportamento-criminale/.*
[51]Cfr., JOHNSON Shane D., SUMMERS Lucia, & PEASE Ken, *Offender as Forager? A Direct Test of the Boost Account of Victimization,* in *J. Quant. Criminol,* 2009, 181-184, 25.

vicina a quella presso cui c'è stato il furto o la medesima)[52].In sostanza, il successo iniziale derivante dal primo crimine, ossia il fatto ad esempio di non essere stato scoperto, convince il criminale a contrassegnare l'area come ''sicura'' per fenomeni delinquenziali futuri del medesimo tipo e così il crimine aumenta fino a renderla un'area c.d. ''rischiosa''[53].In uno studio, i ricercatori hanno scoperto che il 76% dei ladri intervistati tendeva a tornare allo stesso posto (a volte la stessa casa)fino alla cattura[54].

Le strategie di polizia basate sul luogo si sono evolute, per questo, in strategie basato sulla teoria criminologica[55]. Per decenni, la ricerca sulle scienze sociali ha influenzato lo sviluppo della polizia basata sui c.d. *hotspot* (lett. ''zone calde''), quindi basata sui luoghi fisici in cui si è verificato il crimine. Basandosi su queste strategie e sulle tecniche già consolidate di utilizzo dei computer per mappare i "punti caldi" del crimine, Brantingham e i suoi colleghi hanno utilizzato la raccolta di dati delle statistiche sulla criminalità per rendere operative queste teorie[56]. Sulla base di queste ricerche, nel futuro, i modelli di criminalità in qualsiasi città potrebbero potenzialmente essere mappati, così visualizzati e, con l'aiuto di un algoritmo di *post-shock*, previsti su base giornaliera[57].

Si è data così vita a un progetto con il dipartimento di polizia di Los Angeles (*LAPD*)[58] e, con l'incoraggiamento dell'allora capo William Bratton e dell'allora capitano Sean Malinowski, la *Foothill Division* della polizia di Los Angeles ha iniziato a testare se la polizia predittiva potesse funzionare nel

---

[52]Cfr., BERNASCO Wim, *Them Again? Same-Offender Involvement in Repeat and Near Repeat Burglaries*, in *Eur. J.Criminol*, 2008, 411-412, 5; FERGUSON Andrew Guthrie, *Predictive Policing and Reasonable Suspicion*, in *Emoryl.J*., 2012, 259- 274-276, 62.
[53]Cfr., JOHNSON Shane D., SUMMERS Lucia, & PEASE Ken, *Offender as Forager? A Direct Test of the Boost Account of Victimization,* in *J. Quant. Criminol*, 2009, 181-184, 25.
[54]Cfr., JOHNSON Shane D. et al., *Space-Time Patterns of Risk: A Cross National Assessment of Residential Burglary Victimization*, in *J.Quant. Criminol*, 2007, 201-203-204, 23
[55]Cfr., HARRIES Keith, *Natl Inst. of Justice, mapping crime: principle and practice*, 1999, 92 e 94; ANSELIN Luc et al., *Spatial Analyses of Crime,* in *4 Criminal Justice, 2000; Mbasurement and analysis of crime and justice* ,2000, 213 e 215; CHAINEY Spencer & RATCLIFFE Jerry, *Gis and crime mapping* , 2005, 8; PAULSEN Derek J. & ROBINSON Matthew B., *Crime mapping and spatial aspects of crime*,2d ed., 2009, 154.
[56]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 66.
[57]*Ibidem.*
[58] Si veda il paragrafo 1, Capitolo II.

mondo reale[59].Il progetto è stato creato proprio per testare se l'algoritmo di Brantingham potesse ridurre i crimini contro la proprietà (furto con scasso, il furto di automobili e il furto da automobili). Le aree mirate sono state, così, identificate intorno alla *Foothill Division* a nord del centro di Los Angeles[60]. Gli agenti avevano istruzioni per pattugliare quelle aree quando non rispondevano alle richieste di servizio o gestivano altre priorità. L'obiettivo espresso era quello di mettere sotto il controllo costante della polizia i luoghi rischiosi per scoraggiare la tentazione della "ripetizione vicina"*(''near repeat'*), quindi per evitare che i criminali commettessero di nuovo reati dello stesso tipo, nelle stesse aree; l'obiettivo era quindi una complessiva riduzione della delinquenza.

Un progetto pilota iniziale nel 2011 ha mostrato una riduzione del 25% dei furti con scasso[61], e anche altri crimini mirati a talune aree sono diminuiti. Improvvisamente, l'idea che un algoritmo informatico potesse prevedere e prevenire il crimine divenne un fenomeno nazionale in tutti gli Stati Uniti.

Quasi immediatamente dopo, la polizia predittiva è passata da un'idea a una realtà e poi a una società for-profit. La rivista Time ha dichiarato, all'epoca, l'algoritmo di polizia predittiva una delle migliori cinquanta invenzioni dell'anno[62].

A partire da questo progetto, dopo innumerevoli fondi forniti dal *Department of Justice*, anche altre città più piccole come Santa Cruz[63], in California, promossero la tecnologia[64]. Le storie di notizie sul New York Times e altre importanti pubblicazioni nazionali e internazionali hanno attirato un aumento dell'attenzione dei media[65] e *PredPol* ha iniziò a commercializzare

[59]Cfr., RUBIN Joel, *Stopping Crime before It Starts*, in *L.A. Times*, 2010; BEAM Christopher, *Time Cops: Can Police Really Predict Crime before It Happens*?, in *Slate*, 2011, *www.slate.com.*; BEISER Vince, *Forecasting Felonies: Can Computers Predict Crimes of the Future*?, in *Pacific Standard*, 2011, 20, *http://psmag.com.*

[60]Cfr., MENDELSON Aaron, *Can LAPD Anticipate Crime with Predictive Policing*?, in *Calif.Rep*., 2013, *http://audio.californiareport.org.*

[61]Cfr., TALBOT David, *L.A.Cops Embrace Crime Predicting Algorithm,* in *Mit Tech. Rev*., 2012.

[62]Cfr., GROSSMAN Lev et al., *The 50 Best Inventions of the Year,* in *Time*, 2011, 55 e 82.

[63] Si veda il paragrafo 1, Capitolo II.

[64]Cfr., STUART Tessa, *The Policemen's Secret Crystal Ball*, in *Santacruz Wkly*, 2012, 9.

[65]Cfr., GOODE Erica, *Sending the Police before There's a Crime*, in *N.Y. Times*, 2011; *Predictive Policing: Don't Even Think about It*, in *Economist*, 2013, 24 e 26.

l'idea che la tecnologia di riduzione criminale mirata e basata sul luogo fosse la ‘’risorsa che ogni dipartimento di polizia doveva avere’’[66].

Sulla scorta di *Predpol* anche altre aziende hanno adottato approcci simili ma con algoritmi più complessi con lo stesso obiettivo di base: mappare i modelli di criminalità utilizzando sistemi di dati predittivi (*big data*) nel tentativo di ridurre il rischio di criminalità[67].

3. Il crimine è prevedibile?

Come si è detto nei precedenti paragrafi, gli algoritmi predittivi utilizzano i ‘’*big data*’’ per creare una mappatura della personalità di alcuni soggetti e sulla base delle loro frequentazioni, del loro ambiente familiare, del luogo in cui vivono (se si tratta di quartieri con alta percentuale di delinquenza o meno), del loro carattere, delle loro attitudini, dei loro interessi ed altri indicatori, individuano una percentuale di rischio di commissione di reati da parte di tali specifici individui, ovvero si individuano i *crime hotposts*. Ci si chiede quindi se il crimine in sé per sé sia prevedibile o meno.

C'è un forte *corpus* di prove a sostegno della teoria secondo cui il crimine è prevedibile in senso c.d. statistico; questo perché i criminali tendono tendenzialmente ad operare nella loro zona di comfort; quindi, tendono a scegliere gli stessi luoghi come *locus commissi delicti*, quelli reputati da loro come ‘’sicuri’’.

Questo si traduce nella commissione dello stesso tipo di crimini che hanno commesso con successo in passato e, generalmente alla stessa ora e nello stesso luogo. Anche se questo fenomeno non accade sempre, si verifica con una frequenza sufficiente per far funzionare ragionevolmente questi metodi.

Secondo il già citato antropologo Jeff Brantingham[68], professore presso l'Università della California (Los Angeles), che ha aiutato a supervisionare il progetto pilota di polizia predittiva nel dipartimento di polizia di Los Angeles

[66]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 67.
[67]*Ibidem.*
[68]V. paragrafo 1 e 2, Capitolo II.

(*LAPD*): ‘’I comportamenti umani non sono così casuali come pensiamo…In un certo senso, il crimine è solo un processo fisico, e se riesci a spiegare come si muovono i colpevoli e come si mescolano con le loro vittime, puoi capirne il funzionamento di una quantità incredibile’’[69].

Le osservazioni di Brantingham sono supportate dalle principali teorie del comportamento criminale, come la teoria dell'attività di *routine*, la teoria della scelta razionale e la teoria del modello criminale[70]. Per lo studio sulla previsione del crimine si è così sviluppata una teoria c.d. mista. Tale teoria prevede che: (i) i criminali e le vittime seguono modelli di vita comuni; le sovrapposizioni in questi modelli indicano una maggiore probabilità di reato; (ii) le caratteristiche geografiche e temporali influenzano il dove e il quando di questi modelli; (iii) man mano che si muovono all'interno di questi schemi, i criminali prendono decisioni "razionali" sull'opportunità di commettere reati, tenendo conto di fattori quali l'area, l'idoneità dell'obiettivo e il rischio di essere scoperti[71].

Identificando e analizzando questi modelli e fattori del comportamento criminale, è possibile, quindi, adottare strategie tattiche di polizia predittiva volte addirittura a guidare le decisioni dei criminali per prevenire la commissione dei crimini. In altre parole, le forze dell’ordine potrebbero adottare metodologie tali da dissuadere il criminale dal delinquere, ad esempio controllando maggiormente le aree ‘’a rischio’’, mostrando così ai futuri criminali un comportamento attivo di supervisione.

La teoria mista si adatta meglio areati come rapine, furti con scasso e furti ed è meno applicabile (perché meno efficace) a reati come la violenza relazionale, che a causa del coinvolgimento di connessioni umane-emotive e comportamenti irrazionali, sono spesso imprevedibili e non rientrano, così, nei tradizionali quadri di "scelta razionale criminale"[72]. Per sopperire a questa

[69]Cfr., RUBIN Joel, “*Stopping Crime Before It Starts,”* in *Los Angeles Times*, 2010.
[70]Cfr., CLARKE Ronald V. and FELSON Marcus, eds., *Routine Activity and Rational Choice, New Brunswick*, in *H.J. Transaction Publishers*, 2003, (*criminal behavior theories*).
[71]Cfr., PERRY Walter L., MCINNIS Brian, PRICE Carter C., SMITH Susan C., HOLLYWOOD John S., P*redictive Policing, The Role of Crime Forecasting in Law Enforcement Operations*, in *Rand Corporation*, Santa Monica, 2013, 2 e 3.
[72]*Ibidem.*

lacuna, sono in fase di sperimentazione anche teorie alternative per spiegare il meccanismo che conduce a comportamenti violenti, portando allo sviluppo di strumenti e metodi per la valutazione dei rischi anche in questi ambiti[73].

4.1 Il '' *Crime Prevention System* ''

Nel 1997 il Congresso degli Stati Uniti scrisse una relazione che si basava su una revisione sistematica di oltre 500 valutazioni scientifiche di pratiche di prevenzione della criminalità, concludendo che alcuni programmi funzionavano efficacemente, altri meno. Già l'anno prima, nel 1996, si discuteva a proposito di determinati temi di allarme sociale quali la delinquenza giovanile, l'abuso di sostanze stupefacenti da parte dei minori, le numerose bande criminali disseminate in tutte le città e altri fattori ad alto rischio, senza però aver trovato una soluzione efficace volta alla loro repressione. Si mirava, quindi ad una complessiva riduzione dei fenomeni delittuosi partendo da una politica repressiva nelle scuole e negli ambienti familiari a ''rischio''. Per questo, qualche tempo dopo, il *National Institute of Justice,* in collaborazione con il Dipartimento di Criminologia e Giustizia Penale dell'Università del Maryland ha studiato un programma di prevenzione al crimine, il c.d. *''Crime Prevention Program''.* Sono stati così divisi, in base a dati statistici, i settori in cui era necessario intervenire per fronteggiare il problema delinquenza, migliorando l'azione del sistema giudiziario. Questi erano: le comunità, le famiglie, le scuole, i mercati del lavoro, il contesto aziendale, tattiche strategiche della polizia, le carceri[74].

Il problema del programma fu quello della scarsità di dati su cui basare una strategia efficace e la mancanza di confronti scientifici comprovati, soprattutto di tipo pratico, tali da determinarne il successo, sussisteva anche la questione

[73]*Ibidem.*
[74]Cfr., AHLSTROM, WINTON, and HAVIGHURST Robert J. (1982). "*The Kansas City Work/Study Experiment.*" in SAFER DANIEL J., (a cura di), *School Programs for Disruptive Adolescents. Baltimore, Maryland: Univer- sity Park Press.*

sulle modalità relative alla quantificazione del ''rischio''[75]. Di fatti ogni valutazione, prettamente teorica, spesso rischia di scontrarsi con la realtà, dove la sua applicazione risulta difficoltosa. Successivamente, per migliorare la forza attuativa del programma, tramite il *Maryland Scale of Scientific Method*[76], un sistema che quantifica l'affidabilità delle analisi su una scala da uno a cinque, sono stati esaminati tre fattori: (i) il controllo delle variabili criminose, (ii) l'impatto degli eventuali dati erronei, e il tasso statistico di criminalità con altri fattori che potrebbero inficiare la forza applicativa del sistema preventivo. In un secondo momento è stata effettuata una comparazione con le precedenti modalità predittive suddividendo la ricerca in più livelli riguardanti, ad esempio, la correlazione tra un programma preventivo e i fattori di rischio associati ad un determinato crimine, gli eventuali impatti rieducativi[77] conseguenti ad un intervento mirato nella comunità della polizia, quale pattugliamento in aree di rischio, piani di sensibilizzazione nelle scuole ecc[78]. Nonostante queste indagini, i fenomeni delittuosi non si sono attenuati.

A Manhattan svariati anni successivi, il procuratore distrettuale, tentò di sviluppare un meccanismo preventivo volto alla repressione delinquenziale, sviluppando il *''Crime Prevention System''*[79], un sistema in grado di tracciare i modelli di reato che si verificano più di frequente in città, associando il *crimen* al *locus commissi delicti*, e indirizzando, così, le forze dell'ordine ad un maggiore controllo delle c.d. aree di ''rischio'' (ossia quelle in cui si verificano, statisticamente, più fenomeni criminosi). Il programma è in grado, ulteriormente, di creare dei veri e propri database, usufruibili dal Pm, o in

[75]Cfr., ANDREWS, D.A., ZINGERI., HOGE R.D., BONTAJ., GENDREAUP., and F.T., "*Does Correctional Treatment Work? A Clinically Relevant and a Psychologically Informed Meta-Analysis*." In *Criminolog* , 1990, 28:369–404.
[76]Cfr., TAXMAN, FAYE, and SPINNER David L. "*The Jail Addiction Services (JAS) Project in Montgomery County, Maryland: Overview of Results From a 24-Month Follow up Study*.", *Unpublished manuscript Department of Criminology and Criminal Justice, University of Maryland*, 1996, (a cura di).
[77]Cfr., FO, W.S.O., and O'DONELLC.R., "*The Buddy System: Relationship and Contingency Conditioning in a Community Intervention Program for Youth With Non- professionals as Behavior Change Agents.*", in *JOURNAL OF CONSULTING AND CLINICAL PSYCHOLOGY,* 1974, 163–69.
[78]Cfr., CROW, W.J., and BULL J.L. (1975). *Robbery Deterrence: An Applied Behavioral Science Demonstration—Final Report. La Jolla, California: Western Behavioral Sciences Institute, and "The Buddy System: Effect of Community Intervention on Delinquent Offenses*.", in *BEHAVIOR THERAPY*, (a cura di), 1975, 522–524.
[79] V. paragrafo 7.1, Capitolo I.

generale dalla p.g., a fini investigativi, ove sono catalogati tutti gli eventi criminali con l'associazione immediata della zona geografica di riferimento. Il piano è stato di grande aiuto per le attività poliziesche sia di routine, sia relativamente ai procedimenti penali in corso e resta uno strumento di grande aiuto relativamente attività della giustizia in generale.

4.2 I diversi modelli di funzionamento dei sistemi di polizia predittiva

È possibile affermare che la previsione del crimine, utilizzando la intelligenza artificiale, sia uno strumento efficace messo a disposizione dei dipartimenti di polizia che, grazie ad algoritmi elaborati da esperti del settore, riesce ad individuare il tempo e il luogo di un probabile crimine e, successivamente, scoprirne la causa, i motivi e la potenziale vittima.

I progetti di *predicitve policing*[80], utilizzano, infatti, dati storici, in genere relativi ad un passato molto recente, che vengono incrociati, utilizzando algoritmi matematici al fine di evidenziare dei comportamenti criminali, che possano aiutare ad individuare e prevedere i futuri possibili reati. Le tecniche predittive [81] utilizzate dalla polizia possono essere divise in quattro classi: (i) tecniche di analisi statistica classiche[82]che utilizzano modelli multivariati basati su regressioni e in generale tecniche supervisionate oltre a modellistica basata sulle *time-series* con procedure di destagionalizzazione annesse[83];(ii) metodi semplici che si basano su indici e *check lists* e non richiedono calcoli complessi; (iii) applicazioni complesse che rientrano in questa categoria i modelli *near-repeat,* e richiedono per la loro elaborazione complicate tecniche computazionali, oltre ad una enorme mole di dati; (iv) metodi personalizzati: che utilizzano tecniche e metodi statistici già sperimentati, che, tuttavia,

[80]Cfr., FERGUSON Andrew Guthrie, *Predictive Policing and Reasonable Suspicion,* 2012.
[81]Cfr., DI NICOLA A, ESPA G, BRESSAN S, DICKSON M, NICOLAMARINO A, *Metodi statistici per la predizione della criminalità. Rassegna della letteratura su predictive policing e moduli di data mining.*, 2014.
[82]Cfr., MASTROBUONI G., *Crime is Terribly Revealing: Information Technology and Police Productivity*, 2014.
[83]Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale* (ricerca scientifica Università Roma Tre), Roma, 2020, ,57 e 65.

vengono adattati ad esigenze specifiche, richieste dalla polizia predittiva caso per caso. Tipici sono, altresì, i modelli e metodi di *machine-learning*, utilizzati per la elaborazione delle *heat maps*.

L'obiettivo di tutti questi metodi è quello di individuare il luogo e il tempo in cui potrebbe essere commesso un crimine.

Più dettagliatamente, per individuare il luogo del reato, viene utilizzata la *hot-spot analysis*[84] una tecnica utilizzata dagli analisti dei vari Dipartimenti di polizia, che, esaminando le azioni criminose passate, si riesce ad individuare le zone a più alto rischio di delinquenza. A tale scopo, vengono utilizzate tecniche predittive come la *grid mapping* e i *covering ellipses*, oltre a metodi di misurazione basati su stime di densità Kernel.

Con la tecnica predittiva della *grid maps,* attraverso l'uso di coordinate cartesiane, si divide un'area oggetto di analisi, in tante celle e si cerca di intercettare e classificare tutti i reati commessi nelle singole partizioni, per individuare le cosiddette "zone calde". Sulla mappa elaborata, è possibile visualizzare i c.d. raggruppamenti ellittici (*covering ellipses*) definiti *clusters* che definiscono le zone calde e le zone ad esse limitrofe. L'algoritmo più usato per segnalare geograficamente i crimini, si tratta del c.d. *nearest neighbor hierarchical clustering (NNHC).*

Vi sono poi modelli analitici basati sul *near-repeat* che riescono a predire il luogo esaminando solamente i dati dei crimini, grazie all'utilizzo di tecniche di predizione di *self-exciting point process* e *pro map*. Questi modelli si basano sulla *multi-vittimizzazione*[85], una teoria molto seguita in criminologia, secondo la quale i soggetti che hanno subito, nel passato, dei reati personali o contro il loro patrimonio, hanno più probabilità di subirne in futuro. Così, come, con molta probabilità, i crimini futuri si verificheranno nello stesso luogo e nelle stesse ore in cui furono commessi i reati passati, i soggetti lesi dal reato rischieranno di essere lesi una seconda volta e così via. Gli analisti hanno infatti evidenziato che, ad esempio, relativamente ai furti di appartamento, vi sono

[84]Cfr., LEIGH Johanna M., DUNNETT Sarah J., and JACKSON Lisa M., *Predictive Policing Using Hotspot Analysis*, Hong Kong, 2016.
[85]Cfr., MURATORE M.G., *La misurazione del fenomeno della criminalità attraverso le indagini di vittimizzazione*, 2011.

complessi residenziali a più alto rischio, rispetto ad altri. Questo fenomeno può derivare o dal fatto che questi individui posseggono abitazioni tali da essere più facilmente aggredibili, (finestre basse, serrature facilmente forzabile, scarsa luminosità o degrado ecc.) o per il comportamento degli abitanti (assenza dalla casa per molte ore al giorno). Lo studio ha evidenziato, altresì, la probabilità con cui i furti potrebbero avvenire nelle zone limitrofe ed in seguito, per questo motivo, è stato elaborato l'*algoritmo di self exciting*, che prevede una mappatura delle zone divise in celle, e che stima, mediante lo studio del *background* criminoso antecedente, un tasso di delinquenza che sale o scende a seconda che venga commesso o meno un crimine nell'area di vicinato segnalata come ''rischiosa''. L'algoritmo si è rivelato molto utile nella prevenzione dei reati contro la proprietà, consentendo anche di individuare i momenti della giornata in cui era più probabile che i crimini si sarebbero verificati (martedì e giovedì tra le 17.00 alle 20.00[86]). Grazie al suo utilizzo si è registrata una riduzione dei crimini pari al 23%.

Per individuare il tempo e, cioè il momento in cui un evento criminale potrebbe essere compiuto, si utilizzano dati storici e dati temporali, grazie ai quali è possibile creare modelli predittivi come le *heat maps*, gli *additive models* o i *modelli predittivi geo-spaziali*, che valutano dati geografici in cui con più facilità potrebbero essere commessi dei reati.

Le *heat maps*, sono delle tabelle che mostrano la densità dei crimini attraverso l'intensità di un colore e che registrano, data, ora, e condizioni degli stessi.

I modelli predittivi geo-spaziali sono sostanzialmente due: la *risk terrain analysis*, che, nella previsione dei reati analizza i tratti geografici di una regione, dividendola in celle e, la *risk terrain modeling* che individua il luogo specifico in cui un reato può essere commesso o ricommesso (stazioni, metropolitane, negozi di alcolici …).

4.3 Sistemi di individuazione degli *hotspots*

[86] Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale* (ricerca scientifica Università Roma Tre), Roma, 2020, 57 e 65.

Per sistemi di individuazione degli *hotspots* si intendono quei *software* finalizzati all'identificazione dei luoghi e dei tempi (data, ora, periodo dell'anno) in cui le probabilità di commissione dei crimini sono maggiormente elevate[87]. Ci sono alcuni algoritmi di estrema rilevanza nelle operazioni di polizia predittiva, tra questi è necessario citare: *RTM, Predpol, X-LAW.*

Il *Risk Terrain Modeling* (*RTM*) è un algoritmo molto utilizzato per la predizione di reati di spaccio di sostanze stupefacenti in determinate aree urbane[88]. I ricercatori, esaminando dati legati alle aree a rischio connesse alla commissione dei reati, come presenza di luminarie stradali scarse o non funzionanti, vicinanza di locali notturni, fermate di mezzi pubblici, stazioni ferroviarie, snodi di strade ad alta percorribilità, sportelli bancomat, compro-oro, parcheggi e scuole e, sottoponendo le informazioni raccolte all'algoritmo *RTM*, sono riusciti ad individuare, nell'ambito di grandi aree metropolitane, delle zone cosiddette "calde" dove il reato di spaccio di sostanze stupefacenti, risultava più diffuso. Questa indagine è molto importante perché grazie ad essa, nell'ottica di una giustizia preventiva e predittiva, è stato possibile intervenire sui luoghi ad alto rischio, per attuare interventi di prevenzione dei reati connessi allo spaccio di sostanze stupefacenti[89].

PredPol, invece, è un *software,* già in uso da alcuni anni negli Stati Uniti e nel Regno Unito, originariamente elaborato da alcuni ricercatori dell'UCLA (Università della California di Los Angeles) in collaborazione con la polizia locale, ora commercializzato da una azienda privata, ed è finalizzato all'individuazione degli *hotspots* (punti ''caldi) relativi al luogo in cui più spesso avvengono determinati reati. La differenza con *RTM* è che non si limita a quelli collegati allo spaccio.

---

[87] Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale* (ricerca scientifica Università Roma Tre), Roma, 2020, 65.

[88]Cfr., In argomento, v. KENNEDY L.W., CAPLAN J.M., PIZAE.L, *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.**;** CAPLAN J.M., KENNEDY L.W., *Risk Terrain Modeling: Crime Prediction and Risk Reduction***,** in UNIV. OF CALIFORNIA PRESS (a cura di), 2016**;** CAPLAN J.M., KENNEDY L.W., BARNUM J.D., PIZAE.L, *Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis to Explore the Dynamics of Criminogenic Behavior Setting*, in *Journal of Contemporary Criminal Justice*, 33, 2017, 133 ss.

[89]*Ibidem.*

Il sito di *PredPol* utilizza solo tre tipologie di dati – tipo di reato, data/ora del reato e luogo del reato – per fare previsioni. La sua tecnologia è stata di grosso aiuto perché ha consentito agli uffici di polizia di ridurre enormemente il tasso di criminalità in varie giurisdizioni degli Stati Uniti ed anche all'estero. In particolare, a Los Angeles è stato registrato un calo del 20% dei reati; nella contea di Jefferson le rapine si sono ridotte del 24%, i furti con scasso che hanno registrato una riduzione del 13%; nel New Jersey, le rapine si sono ridotte del 54% ed i furti di auto hanno avuto una riduzione del 69% [90].

Da ultimo il software *X-LAW* è uno strumento usato dalla polizia italiana, originariamente predisposto dalla Questura di Napoli, che si basa su un algoritmo capace di rielaborare una mole enorme di dati estrapolati dalle denunce inoltrate alla Polizia di Stato per individuare una serie di reati[91].

L'algoritmo, esaminando fattori ricorrenti o coincidenti, consente non solo di individuare i soggetti ad alto rischio, ma anche di individuare le zone più pericolose, al fine di attuare interventi delle forze dell'ordine con lo specifico scopo di impedire la commissione di altri reati e anticipare le azioni criminose, anche mediante interventi che consentano di cogliere in flagranza gli autori dei potenziali reati[92].

4.3.1 Il *software PREDPOL*

PredPol è un software creato una azienda privata che ha guidato le nuove tecnologie di polizia predittiva, segnalando agli agenti i luoghi a rischio di criminalità e i momenti della giornata in cui è più probabile che avvengano attività delittuose[93]. L'azienda si è espansa rapidamente e ha sviluppato un marchio forte nel campo del *predictive policing*. Lo scopo è quello di indirizzare la polizia verso le località previste come rischiose, portando così ad una riduzione della criminalità.

---

[90]Cfr., *https://www.predpol.com/*, visitato il 9 agosto 2019.
[91]Cfr., Notizie riferite da IASELLI M., *X-LAW: la polizia predittiva è realtà*, in *Wired.it*,2019; PARODI C., SELLAROLI V., *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto penale contemporaneo*, fasc.VI, 2019, 56. Per una descrizione di Keycrime, fornita dal suo stesso ideatore, VENTURI Mario, v. in *Profiling*, 2014, 5, 4.
[92]Cfr., *Ibidem*. Ulteriori informazioni e filmati relativi a X-LAW sono facilmente reperibili *online*.
[93]Cfr., PREDPOL: *Management Team, www.predpol.com/about/company/ [https://perma.cc/3Z76-LSAS]*.

PredPol offre diversi servizi predittivi, ma il più noto prevede le aree di probabile attività criminale incentrate particolarmente su tali fattispecie di reato: furto con scasso e furto di automobili[94].

Il funzionamento è basato su un algoritmo ispirato alla sismologia ed è ispirato dal fatto che alcuni modelli di criminalità seguono schemi ripetitivi simili alle scosse di assestamento dei terremoti. Questo meccanismo viene definito come il c.d. ‘’effetto scossa di assestamento’’ e determina la consapevolezza che, dopo la commissione di un reato, in un determinato luogo, aumenta la probabilità della commissione di altri reati simili, vicini nel tempo e nello spazio, rispetto al reato originario. L'algoritmo di *PredPol* rende operativa questa intuizione anche quando si tratta di prevedere i reati contro il patrimonio, che sembrano seguire, nella prassi, lo stesso schema applicativo.

Gli input che utilizza il sistema di *PredPol* sono le registrazioni sugli incidenti, il tipo rilevato di crimine, l'ora e il luogo[95]. Partendo da queste informazioni, *Predpol* limita le possibili variabili, rilevanti per quantificare le probabilità di reiterazione, restringendo il campo, fino a prevedere veri e propri profili di reati futuri. Gli arresti passati non rientrano nei dati rilevanti per l’analisi ma vengono qualificati esclusivamente come sospetti, restano, invece, rilevanti le denunce giornaliere fatte alla polizia per studiarne la provenienza e quindi l’area associata. Ad esempio, se più di una denuncia segnala reati associati spesso ad una determinata area geografica, diventa rilevante per l’indagine, indirizzando la polizia ad un maggior controllo.

Per cui, questi input vengono analizzati come dati e pongono in evidenza specifici hot-spot (luoghi ‘’caldi’’, quindi a rischio criminalità), previsti su una c.d. *timeline* giornaliera.

PredPol funge, quindi, da sistema di gestione delle pattuglie. Per la polizia, le previsioni basate sui *big data* si trasformano in azioni operative attraverso

---

[94] *Ibidem.*

[95] V., MOHLERG.O. et al., *Self-Exciting Point Process Modeling of Crime*, in *J. Am. Stat.*, 2011, Ass’n 106, 100 ; v. anche *Predictive Policing*: *MOHLER George Interview*, in *Data Sci. Wkly*., *www.datascienceweekly.org/data-scientist-interviews/predictive-policing-george-mohler-interview [https://perma.cc/QF64-K958]*.

mappe generate dal computer in base al crimine previsto e al luogo ad esso associato.

Installati sulle auto della polizia, questi computer generano le c.d. mappe ‘’obiettivo’’, grazie alle quali è possibile prevedere quali aree precise (di grandezza massima di 50 per 50 metri quadrati) rappresentano un rischio elevato di commissione di un particolare crimine[96].

La strategia consiste, quindi, nell'aumentare la presenza e il controllo della polizia in determinati luoghi in determinati orari previsti. *PredPol*, a sua volta, può tenere traccia del tempo che gli agenti trascorrono in un'area tramite dispositivi *GPS* e quindi riferire tali informazioni agli ufficiali di polizia.

Si prevede che tramite una maggiore visibilità delle aree vulnerabili alla criminalità si scoraggerà la delinquenza in quel luogo. Ad esempio, se l’algoritmo prevede che un parcheggio sarà teatro di un furto d'auto, a causa di un’analisi sullo schema di furti d'auto già avvenuti in periodi vicini e nella medesima area, l'invio di un'auto della polizia in quel luogo identificato scoraggerà il potenziale ladro d'auto. L'obiettivo non è tanto quello di arrestare gli individui ‘’rischiosi’’ nell'area, quanto piuttosto mostrare agli eventuali criminali futuri che la polizia è presente e le città non sono fuori dal loro controllo. Lo scopo del modello *Predpol*, quindi, più che aumentare gli arresti, è quello di ridurre le vittime, o più in generale, i potenziali soggetti lesi dal reato[97].

I risultati della strategia di *PredPol*, come tutto il tema del *predictive policing* nel suo complesso, sono oggetto di dibattito. L'esame dei tassi di criminalità nelle aree che hanno implementato la tecnologia di *PredPol* dimostra, infatti, sia successi che fallimenti[98]. Di fatti, nella prassi, gli aumenti della criminalità non possono essere imputati a una particolare tecnologia, così

[96]Cfr., STUART Tessa, *The Policemen’s Secret Crystal Ball, Santa Cruz Wkly*, 2012, 9.
[97]Cfr., THOMAS Emily, *Why Oakland Police Turned Down Predictive Policing, Vice Motherboard*, 2016.
[98]Cfr.,VUONG Zen, *Alhambra Police Chief Says Predictive Policing Has Been Successful*, in *Pasadena Star-News*, 2014; AHUMADA Rosalio, *Modesto Sees Double-Digit Drop in Property Crimes – Lowest in Three Years*, in *Modesto Bee*, 2014; with ALDAX Mike, *Richmond Police Chief Says Department Plans to Discontinue “Predictive Policing” Software,* in *Richmond Standard* , 2015.

come le riduzioni della criminalità non possono essere attribuite ai nuovi modelli informatici.

I fondatori di *PredPol*, ricercatori e scienziati accademici, hanno pubblicato il primo studio *peer-reviewed* sulla tecnologia[99]. Gli studiosi hanno confrontato le capacità di previsione del crimine dell'algoritmo *PredPol* con le indagini degli analisti criminali esistenti e con quelle della polizia. Da tale raffronto, nel corso un'analisi di circa centoventi giorni, emerge che la polizia di un particolare distretto di Los Angeles si è alternata seguendo talvolta la previsione di *PredPol* e altre quella degli analisti criminali, ecco cosa ne è derivato: ''A Los Angeles, gli analisti della criminalità hanno previsto il 2,1% dei crimini e l'algoritmo ha previsto il 4,7% dei crimini... Il modello *PredPol* ha, quindi, dimostrato un'accuratezza predittiva 2,2 più alta[100]''. Un medesimo paragone è stato fatto anche a Kent in Gran Bretagna dove gli analisti del crimine hanno previsto il 6,8% dei crimini, contro il più accurato punteggio/percentuale dell'algoritmo del 9,8%. Anche in questo altro *test*, il sistema *Predpol* ha dimostrato un livello di precisione più elevato, la macchina ha prevalso sulle analisi umane[101].

Sebbene tutti gli studi accademici siano necessariamente limitati, a causa degli scarsi elementi di analisi, vista l'applicazione pressoché recente di questi algoritmi, la conclusione positiva di questa indagine iniziale fornisce alcune prove sull'effettivo funzionamento del *predictive policing*. Se la previsione risulta accurata, condurre la polizia nei posti giusti al momento giusto dovrebbe ridurre il rischio di criminalità.

4.3.2 Il *software HunchLab*

A St. Louis, Missouri, i distretti di polizia hanno adottato una strategia di polizia predittiva per dare priorità alle risorse e professionalizzare le

[99]V., MOHLERG.O. et al., *Self-Exciting Point Process Modeling of Crime*, in *J. Am. Stat*, 2011, Ass'n, 100, 106; V. anche *Predictive Policing:* MOHLER George *Interview*, in *Data Sci. Wkly*., *www.datascienceweekly.org/data-scientist-interviews/predictive-policing-george-mohler-interview [https://perma.cc/QF64-K958]*.
[100]Cfr., FERGUSON, *The Rise of Big Data Policing*, 69 e 70.
[101]Cfr., MOHLERG. O. et al., *Randomized Controlled Field Trials of Predictive Policing*, in *J. Am. Stat. Assoc.*, 2015, 1399, 110.

pattuglie[102]. In collaborazione con una piccola *start-up* con sede a Filadelfia denominata Azavea, il dipartimento di polizia di Jennings, Missouri, ha iniziato a sperimentare un programma di polizia predittiva chiamato ‘’*HunchLab*’’[103].

Il modello *HunchLab* inserisce dati sulla criminalità, dati sul censimento e densità di popolazione e aggiunge altre variabili come la posizione di scuole, chiese, bar, club e centri di trasporto. L'algoritmo, quindi, confronta i dati raccolti inerenti ad un crimine, creando una mappa del rischio costantemente aggiornata dell'area[104].In queste mappe, i crimini vengono differenziati in base a colori, si tratta del c.d. *‘’color coded by crime’’*, e tramite elaborazioni statistiche di pericolosità, il modello calcola le percentuali di probabilità di commissione di attività criminale.

Dal punto di vista tecnologico, *HunchLab* ha costruito dispositivi mobili portatili, simili ai *tablet*, per consentire agli agenti di polizia di vedere in tempo reale le aree da pattugliare e di suggerire agli agenti le tattiche appropriate[105]. I meccanismi di raccolta dei dati comportano sia la trasmissione di informazioni agli agenti sia la raccolta di informazioni dagli agenti sulle loro azioni.

Un ufficiale di pattuglia può, così, vedere, seguendo i colori sullo schermo del dispositivo *HunchLab* se l’area che sta controllando sia ad esempio un'area *high-gun-crime* (quindi un’area ad alto rischio di uso delle armi) o un'area *high-residential-burglary* (quindi un’area con rischio di furto con scasso in abitazione) e preparare in base al rischio di crimine che deve fronteggiare, una adeguata strategia di prevenzione.

Come dettagliato in un'indagine del Marshall Project, queste tecniche di controllo predittivo hanno un impatto diretto sulla polizia e sul cambiamento delle strategie di vigilanza[106].

---

[102]Cfr., FERGUSON A. G., *Big Data’s Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 63.
[103]Cfr., REYES Juliana, *Philly Police Will Be First Big City Cops to Use Azavea's Crime Predicing Software, in Technically Media inc., 2013, http://technical.ly.*
[104]Cfr., HUNCHLAB, U*nder the hood*, 2015.
[105]Cfr., CHAMMAH Maurice, *Policing the Future*, in *The Marshall Project*, 2016.
[106]Cfr., CHAMMAH Maurice, *Policing the Future*, in *The Marshall Project*, 2016, *www.themarshallproject.org*.

HunchLab si definisce, quindi, come un "sistema di gestione delle pattuglie" che combina elementi delle tecnologie sulla base di *PredPol*[107] e *RTM*[108], aggiungendo, però, altri fattori. Il sistema, infatti, prevede le aree di rischio criminale (ad esempio come *Predpol*), ma suggerisce anche alcune tattiche di polizia mirate per affrontare tali rischi. Come altri sistemi, il modello inizia con l'analizzare i dati sulla criminalità e le informazioni che ne derivano per poi ordinarli mediante appositi algoritmi[109].Inoltre, i set di dati che non riguardano prettamente il fenomeno criminale, ma il contesto vengono aggiunti e classificati in base a fenomeni ciclici ed eventi temporali, come ad esempio: stagionalità, giorni della settimana, festività, eventi sportivi, ecc[110]. Il modello include anche informazioni su autori di reati noti, fattori socio-economici e modelli meteorologici[111]. Più variabili sono presenti, più il modello è preciso e complesso, con una conseguente valutazione dettagliata dei rischi e dei benefici derivanti dall'analisi strategica.

HunchLab utilizza tecniche di apprendimento automatico[112] per analizzare i dati sulla criminalità, e testare i dati, confrontando ingenti quantità di set di dati e quindi modellando i dati da utilizzare nelle previsioni. In altre parole, l'algoritmo predittivo di *HunchLab*, più dati analizza, più previsioni elabora, più diventa preciso, addestrandosi autonomamente ad imparare sempre di più sulla base di nuovi processi conoscitivi. Queste previsioni vengono poi trasformate in suggerimenti per il posizionamento nelle città delle pattuglie. I crimini vengono suddivisi e ponderati per severità e associati a efficaci strategie di pattugliamento volte a bilanciare le previsioni criminose (in modo che i reati più gravi abbiano più peso, anche se meno frequenti) con la massima l'efficacia della polizia. Quindi, ad esempio, un crimine armato potrebbe avere

[107]V. paragrafo 4.4.1.
[108]V. paragrafo 4.4.
[109]Cfr., HUNCH LAB, *HunchLab Under the Hood*, 12, *https://cdn.azavea.com/pdfs/hunchlab/HunchLab-Under-the-Hood.pdf.*
[110]Cfr., FERGUSON Andrew Guthrie, *Predictive Policing Theory*: *The Cambridge Handbook of Policing in the United States,* in TAMARA RICE LAVE & ERIC J. MILLER CAMBRIDGE UNIV. PRESS (a cura di), 2019, Capitolo 24, American University, WCL Research Paper, 2020-10 496, *https://ssrn.com/abstract=3516382*.
[111]Cfr., HUNCH LAB, *HunchLab Under the Hood,* (p. 12), *https://cdn.azavea.com/pdfs/hunchlab/HunchLab-Under-the-Hood.pdf.*
[112]V. paragrafo 8, Capitolo I.

un peso di gravità più elevato (a causa del rischio per la comunità) e un'accusa di aggressione aggravata potrebbe avere un peso più basso, dando priorità nell'azione di polizia ai reati più efferati e poi a quelli minori.

Agli agenti di polizia che utilizzano *HunchLab* vengono fornite informazioni su dove pattugliare (in base alle previsioni) e quindi vengono fornite anche tattiche suggerite per migliorare l'efficienza in quelle aree particolari. Queste tattiche si concentrano sulle modalità con cui un agente di polizia dovrebbe interagire con i soggetti ritenuti ''pericolosi'' per combattere un particolare rischio di criminalità, ad esempio, mediante fermi o perquisizioni.

I primi test di *HunchLab* hanno mostrato risultati positivi a Chicago[113] e Filadelfia[114] nella riduzione della criminalità, ma l'algoritmo è destinato ad apprendere sempre di più sulla base dei dati raccolti di volta in volta, per cui sono in via di sviluppo le evoluzioni future del software, non resta altro che aspettare nuovi scenari per scoprirlo.

4.3.3 Il *software X-LAW*

Uno studio accademico effettuato a Napoli, nel 2004, ha sviluppato un algoritmo che ha permesso la creazione del programma predittivo *X-LAW*, un software che consente di prevedere, utilizzando i dati acquisiti dalle denunce fatte alla polizia, ed elaborando mappe virtuali, una percentuale di reati di natura ''predatoria'' come rapine, scippi, borseggi, furti, e reati similari, riuscendo a percepire dove, in quale area, e quanti reati sono stati commessi. Questo sistema informatico è nato da uno studio sui reati commessi negli anni 90, ma è stato perfezionato solo nel 2003, anno in cui è stato anche sperimentato in sei città italiane. Solo nel 2019 tale sistema è stato validato dal Dipartimento di Pubblica Sicurezza Direzione Centrale Anticrimine.

[113]Cfr., FINGAS Jon, *Chicago Police See Less Violent Crime After Using Predictive Code*, in *Engadget*, 2017.
[114]Cfr., REYES Juliana, *Philly Police Will Be First Big City Cops to Use Azavea's Crime Predicting Software*, in *Technically Media Inc*., 2013.

Lo studio, condotto dal prof. Di Gennaro[115], del tutto innovativo in Italia, si basa sull'analisi criminale, cioè su una indagine che verifica le connessioni tra l'evento criminoso, l'autore e il luogo, del reato, al fine di prevenire la commissione di altri crimini[116]. Esistono due tipi di analisi criminale: (i) il *profiling* che esamina l'aspetto psicologico-dinamico e studia maggiormente le variabili che conducono alla commissione di un reato, come la scena del crimine, il movente, il modo di agire e lo stato mentale, con l'intento di acquisire i comportamenti tipici che precedono il reato, unitamente ad anticipare la scena del crimine[117], indagine rivelatasi molto utile soprattutto relativamente al reato di omicidio; (ii) il *crime mapping* che esamina gli aspetti di natura scientifica, e si basa su indagini di natura statistico-geografiche, molto utili nei reati contro il patrimonio, di natura predatoria (furto, rapina, scippo ecc.)[118]. Ad ausilio investigativo, in aggiunta, vengono utilizzati i *GIS* (*Geographic Information System*) che sono dei sistemi matematici che, con l'ausilio di operatori specializzati, producono mappe cosiddette georeferenziate, che indicano la distribuzione dei reati in varie aree urbane e metropolitane.

Il sistema algoritmico *X-LAW* rientra nella categoria del *crime mapping*, rappresentandone, però, una evoluzione dal momento che, aggiunge alle teorie psicologiche, proprie del *crime mapping*, le teorie del *machine learning* derivanti dalla IA; questo ha prodotto, come effetto: la riduzione della percentuale di crimini c.d. predatori, un più efficace controllo del territorio da parte delle forze dell'ordine, e una maggiore fiducia dei cittadini nelle attività delle forze dell'ordine.

Grazie agli ottimi risultati raggiunti, il sistema *X-LAW* è stato adottato anche in altre città, tra cui Parma e Salerno, e si prevede un suo utilizzo e

---

[115]Cfr., DI GENNARO, G., MARSELLI R., LOMBARDO E., SPINA M. *Tolleranza zero o deterrenza selettiva*, in DI GENNARO G. e MARSELLI R. (a cura di), 2018; *Secondo Rapporto Criminalità e Sicurezza a Napoli*, in FEDOA PRESS (a cura di), University Federico II, Napoli.

[116]Cfr., ARAMINI, M. (2002). *I processi inferenziali nel profilo psicologico del criminale. Psicologia&Giustizia*, 2002, 1, 2 s.

[117]Cfr., JACKSON J.L., BEKERIAN, D.A., *Does offender profiling have a role to play*, in JACKSON J. L., BEKERIAN, D. A. (diretto da), *Offender profiling: Theory, research and practice, Chichester*, in WILEY (a cura di), 1997, 1 e 7.

[118]Cfr., UMMARINO A., *Una introduzione ai software per il crime mapping*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, 2013, 147-148, 7.

sviluppo sempre crescente. Restano, tuttavia, alcune criticità legate al fenomeno del *displacement,* cioè lo spostamento delle organizzazioni criminali, in luoghi diversi da quelli previsti dalla IA, che ha ridotto del 10-20% la probabilità di anticipare l'evento criminoso[119].

4.4 Sistemi basati sulla identificazione di individui a rischio: la *Heat List* e l'*HART* (UK), l'*Harm Assessment Risk Tool*

Gli algoritmi predittivi, per quantificare la pericolosità di determinati individui, sono programmati mediante strumenti di valutazione del rischio, i c.d. *risk assesment risk tool*. Tra il 2012 e il 2015, molte associazioni americane, quali l'*American Bar Association*, la *National Association of Counties*, la *Conference of State Court Administrators*, e la *Conference of Chief Justices*, hanno manifestato il loro parere favorevole circa l'uso di tali strumenti alla fase investigativa preventiva e pre-processuale[120]. Già precedentemente, nel 2007, il *National Center for States Courts* aveva incoraggiato questo nuovo sistema procedimentale. Il sistema americano ha così assistito ad un crescente uso di questi nuovi software predittivi basati sul ''rischio'' di delinquenza, al punto da revisionare, nel 2017, il *Model Penal Code* dell'*American Law Institute*, esortando, così, a utilizzare «gli strumenti ''attuariali'' per identificare i soggetti che presentano caratteristiche tali da determinare un particolare rischio per la pubblica sicurezza e per la società[121]». Questi nuovi strumenti, acquisendo e studiando ingenti quantità di dati, quali lo stile di vita, l'ambiente familiare, le attitudini caratteriali, gli ideali politici, la situazione patrimoniale/economica, e le relazioni con la società[122] riescono a creare una vera e propria mappatura della personalità degli individui, tale da determinare chi può incorrere potenzialmente nella commissione di reati. Questi sistemi creano così un vero e proprio profilo personale di individui ritenuti ''rischiosi'' e ne tracciano le attività al fine di segnalare alle forze di polizia, eventuali

[119] v., *https://www.stateofmind.it/2021/03/xlaw-prevedere-reati/*.
[120] V. GARRETTB.L. – MONAHAN J., *Judging Risk, in California Law Review, Forthcoming,* 10 s.
[121] Cfr., *Model penal code: sentencing, Proposed Final Draft*, 2017, 171.
[122] Cfr., KEHL D. – GUO P. – KESSLER S., *Algorithms in the Criminal Justice System,* cit., 11.

comportamenti o movimenti sospetti e teoricamente delittuosi, prima che vengano portati a compimento.

Progettata da Miles Wernick dell'*Illinois Institute of Technology* (IIT), la c.d. *''Heat list''* (lista calda) utilizza undici variabili per creare punteggi di rischio da 1 a 500[123]. Più alto è il punteggio, maggiore è il rischio di essere vittima o autore di violenza armata. L'algoritmo riesce a predire persino chi sarà vittima di una sparatoria. Nelle sperimentazioni l'algoritmo *heat-list* è stato tragicamente accurato[124]. In un violento fine settimana della Festa della Mamma nel 2016, l'80% delle 51 persone colpite è stato correttamente identificato, nel giro di due giorni, nella lista calda di Chicago come potenziale vittima[125]. Nel *Memorial Day* del 2016, il 78% delle 64 persone colpite era nella lista. Tramite la *Heat list*, la polizia ha potuto mirare a sopprimere molti fenomeni criminali, dando la priorità ai fenomeni di violenza giovanile e preservando i soggetti più a rischio di diventare vittime[126].

L'approccio algoritmico della *Heat list* di Chicago basato sulla prevenzione mirata è diventato un esempio importante di polizia dei *big data*. Partendo sul concentrarsi sugli arresti a Kansas City, la *Heat list* è poi cresciuta in complessità allargando i suoi orizzonti applicativi. L'algoritmo rimane segreto, ma è possibile affermare che i fattori, cui si basa l'analisi di *machine-learning*, includono la storia criminale passata, gli arresti, lo stato di libertà condizionale e se il soggetto da controllare è stato mai identificato come parte di una banda criminale[127].

Tutti nelle prime liste hanno avuto qualche coinvolgimento criminale generico con il dipartimento di polizia di Chicago. È stato osservato che "Il software è generato sulla base di dati empirici che elencano le informazioni

---

[123]Cfr., RHEE Nissa, *Can Police Big Data Stop Chicago's Spike in Crime*?, in C*hristian Sci. Monitor* , 2016.
[124]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 37.
[125]Cfr., Editorial, *Who Will Kill or Be Killed in Violence-Plagued Chicago? The Algorithm Knows*, in *Chi. Trib.*, 2016.
[126]Cfr., PAPACHRISTOS Andrew V., Commentary*: CPD'S Crucial Choice: Treat Its List as Offenders or as Potential Victims*?, in C*hi.Ttrib.*, 2016.
[127]Cfr., Chi. Police Dep't, CUSTOM NOTIFICATIONS IN CHICAGO, SPECIAL ORDER, 10-05 III.C, 2015, *http://directives.chicagopolice.org.*

circa le caratteristiche di una personalità criminale, gli eventuali episodi di violenza, anche tra i membri del gruppo criminale, la frequenza delle attività criminali e il grado di intensità, inteso anche come gravità, della storia criminale''[128]. L'algoritmo classifica queste variabili per ottenere un punteggio predittivo, determinando quanto gli individui possano essere definiti "caldi" (hot) in termini di rischio di violenza[129].

La presenza di un soggetto nella *Heat list* può essere determinare una "visita di notifica personalizzata" (*''custom notification visit''*[130])[131].

Questa operazione comporta una visita a domicilio, di solito da parte di un alto ufficiale di polizia, un assistente sociale e altri membri scelti ad hoc per il caso (talvolta persino un allenatore di calcio o un prete). Durante la visita, la polizia consegna una "lettera di notifica personalizzata" (*''custom notification letter''*[132]) che dettaglia le informazioni a sua conoscenza circa il passato criminale dell'individuo, nonché un avvertimento sul futuro"[133]. Come descritto dal dipartimento di polizia di Chicago. ''La lettera di notifica personalizzata sarà utilizzata per informare le persone dell'arresto, dell'accusa o delle conseguenze della condanna che questi soggetti potrebbero affrontare se scelgono o continuano a impegnarsi in attività violente e/o criminali. La lettera verrà scritta specificamente, di volta in volta, per l'individuo identificato come pericoloso e verranno allegati quei fattori noti sull'individuo, tali da definirlo ''rischioso'', inclusi gli arresti precedenti e i potenziali risultati algoritmici di condanna per futuri atti criminali''[134]. Queste lettere di notifica

[128]*Ibidem.*
[129]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press,* 38.
[130]*Ibidem.*
[131]Cfr., Chi. Police Dep't, CUSTOM NOTIFICATIONS IN CHICAGO, SPECIAL ORDER, 10-05 III.C, 2015, *http://directives.chicagopolice.org.*
[132]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press,* 38.
[133]Cfr., GORNER Jeremy, *The Heat List*, in *Chi. Trib.*, 2013.
[134]Cfr., Chi. Police Dep't, CUSTOM NOTIFICATIONS IN CHICAGO, SPECIAL ORDER, 10-05 III.C, 2015, *http://directives.chicagopolice.org.*

personalizzate simboleggiano messaggi formali di avvertimento scritti, con cui si vuole avvisare il soggetto sospettato che è osservato[135].

Anche se le previsioni della *Heat list* ha avuto spesso riscontri oggettivi con la realtà, non mancano questioni dubbie.

Ad esempio, il *Chicago Tribune* ha riportato la storia di Robert McDaniel, un uomo di 22 anni che è stato visitato da un comandante della polizia a casa sua". Come altri sulla lista del caldo, è stato avvertito di evitare un percorso criminale[136]. L'unico problema era che McDaniel non era un criminale ''esperto''. Era stato, infatti, condannato, solo una volta, per un reato non particolarmente grave, ma era stato comunque inserito nella *Heat list*. Quando ha chiesto le motivazioni alla base di una classificazione (intesa come punteggio di rischio) così alta da giustificare una visita delle forze dell'ordine, è stato informato che la sua menzione nella lista derivava dalla morte della sparatoria del suo migliore amico un anno fa[137]. In altre parole, la sua perdita personale ha aumentato il suo rischio di violenza, secondo l'algoritmo.

Altri individui sono indicati nella lista per ragioni più ovvie. Il New York Times ha profilato la morte dell'aspirante rapper Young Pappy, alias Shaquon Thomas, un giovane di 19 anni che era stato arrestato numerose volte, e al momento della sua morte era coinvolto in una faida tra bande in corso[138]. Il punteggio della *heat-list* di Young Pappy era 500+ (il numero più alto) e la previsione si è rivelata tragicamente accurata 38 e purtroppo è stato colpito poche settimane prima di ricevere una visita di notifica personalizzata.

L'algoritmo alla base della *Heat list* di Chicago è stato il primo vero e proprio modello di previsione basato sulla persona e la città ha svolto il ruolo di laboratorio per i primi test. Come ha dichiarato pubblicamente il comandante della polizia di Chicago Jonathan Lewis, l'algoritmo della *Heat-list* "diventerà una *best practice* nazionale''. Ciò informerà i dipartimenti di polizia di tutto il

[135]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 38.
[136]Cfr., GORNER Jeremy, *The Heat List*, in C*hi. Trib*., 2013.
[137]Cfr., DAVEY Monica, *Chicago Police Try to Predict Who May Shoot or Be Shot*, in *N.Y. Times*, 2016.
[138]*Ibidem.*

Paese e di tutto il mondo sugli utilizzi più efficaci della polizia predittiva per risolvere i problemi, in primis quello di salvare vite umane[139].

Nonostante le previsioni algoritmiche, la polizia predittiva di Chicago ha dovuto scontrarsi con una spiacevole realtà: la violenza è solo aumentata.

In effetti, il 2016 ha assistito ad impreviste e strazianti sparatorie violente che hanno condotto a numerose critiche del modello[140]. Restano, quindi, domande sull'efficacia del programma e in particolare sul se basti per porre rimedio ai rischi sociali ed economici identificati. Ad esempio, esiste la questione aperta riguardante la capacità o meno dell'algoritmo di distinguere adeguatamente tra obiettivi che sono "ad alto rischio" (coloro che potrebbero essere fucilati) e quelli che sono "ad alta minaccia" (coloro che potrebbero sparare)[141]. La sorveglianza intensiva e l'intervento della polizia per coloro che potrebbero essere vittime potrebbero non essere abbastanza per proteggerle. Il problema nasce dal fatto che la formula di programmazione *heat-list* eguaglia il rischio ideale e la minaccia concreta, non distinguendone la pericolosità, conducendo le risorse di polizia ad incorrere in errori di valutazione.

Nel 2016, la *RAND Corporation*, una organizzazione senza scopo di lucro ha esaminato lo schema di funzionamento di base del sistema di *heat-list* relativo agli arresti fondati su sospetti nascenti dall'attività dei social network[142]. *RAND* ha scoperto che la *Heat list* mostrava una scarsa accuratezza predittiva. Il sistema ha rivelato che su 426 nomi "caldi" (''hot''), poche previsioni erano accurate[143].

Come ha riferito il *RAND*: "Il risultato principale, derivante da questo studio, è che nel sistema *heat list* non c'era più distinzione tra le probabilità di rischio o di pericolo in concreto per gli individui, di delinquere o di essere

---

[139]Cfr., STROUD Matt, *The Minority Report, Chicago's New Police Computer Predicts Crimes, but Is It Racist*? In *Verge*, 2014, *www. theverge.com.*
[140]Cfr., DAVE Monica, *Chicago Has Its Deadliest Month in About Two Decades*, in *N.Y. Times*, 2016.
[141]Cfr., FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017, 7 e 19, in *NYU Press*, 39.
[142]Cfr., SAUNDERS Jennifer, HUNT Priscilla, & HOLLYWOOD John S., *Predictions Put into Practice: A Quasi-Experimental Evaluation of Chicago's Predictive Policing Pilot*, in J. *Experimental Criminol.*, 2016, 347-355-364, 12.
[143]*Ivi*, 363.

vittime di determinati crimini, a seguito della analisi SSL (*Strategic Suspects List*). Ciò trova conferma nel fatto che la tendenza degli omicidi della città non era coerente con l'analisi algoritmica.''[144].

Tuttavia, due importanti intuizioni nascono dall'esperienza *heat-list*. In primo luogo, l'approccio di salute pubblica di mappare le reti sociali pericolose può identificare con successo coloro che potrebbero essere coinvolti nella violenza. Infatti, seppure lo studio *RAND* abbia mostrato che la *heat list* 1.0 non sembrava avere successo, da allora il modello predittivo si molto è evoluto[145]. Il dipartimento di polizia di Chicago, invero, ha riferito che "Dal 2016 in poi, più del 70 per cento delle persone che sono state vittime di un crimine a Chicago erano nella lista, così come più dell'8 per cento degli individui, presenti nella lista, perché segnalati come pericolosi, sono stati arrestati in relazione ad alcune sparatorie avvenute in città''[146] Questi sviluppano dimostrano previsioni incredibilmente accurate.

In secondo luogo, studiare i dati per prevedere chi potrebbe essere impegnato nella criminalità non pone automaticamente fine alla violenza, quindi misurare l'efficacia di un algoritmo sulla base della completa eliminazione del crimine sarebbe fallimentare. Le notifiche personalizzate, ad esempio, potrebbero non avere l'effetto previsto se non implementate con particolare attenzione nell'affrontare i bisogni sociali collegati ai fenomeni di delinquenza. Si tenga conto che solo da poco tempo l'algoritmo è diventato un meccanismo di *targeting* predittivo per la polizia. Mappare la rete sociale della violenza, quindi è più facile che porre fine alla violenza, ma è un inizio per una efficace lotta alla delinquenza.

L'*Harm Assessment Risk Tool* (*HART*) è uno dei più importanti modelli di «*machine learning tool*»[147]che viene utilizzato per quantificare la pericolosità

[144]*Ivi,* 364.
[145]Cfr., DAVEY Monica, *Chicago Police Try to Predict Who May Shoot or Be Shot,* in *N.Y. Times,* 2016; V. anche PAPACHRISTOS Andrew V., Commentary: *CPD'S Crucial Choice: Treat Its List as Offenders or as Potential Victims*? ,in *Chi. Trib.* , 2016; V. altresì, RHEE Nissa, *Study Casts Doubt on Chicago Polices Secretive "Heat List"* in *Chi. Mag.*, 2016.
[146]Cfr., DAVEY Monica, *Chicago Police Try to Predict Who May Shoot or Be Shot*, in *N. Y. Times,* 2016.
[147]Cfr., URWIN S., *Written evidence submitted by Sheena Urwin, Head of Criminal Justice, Durham Constabulary*, in *www.parliament.uk*, 2018.

di un determinato individuo e/o per verificare il rischio che un soggetto arrestato commetta nuovi reati (di diversa o medesima specie) nell'arco dei due anni successivi alla liberazione. Il programma ha come obiettivo, quello di ridurre il rischio di recidiva [148] e di individuare i soggetti che possono essere inseriti in un programma di recupero, chiamato *Checkpoint*, che costituisce una valida alternativa all'esercizio dell'azione penale[149]. L'analisi dei dati riesce ad individuare e, quindi a catalogare, le persone ad alto o basso rischio per valutare se le stesse potranno commettere, in futuro, un reato grave, come l'omicidio, o un reato di minore entità. Il sistema può anche aiutare a prevedere l'assenza di rischio alla commissione di reati. Tuttavia, il programma Checkpoint viene utilizzato, nella prassi, esclusivamente per gli individui che possono commettere reati meno gravi e quindi a basso rischio [150].

Il sistema *HART* nasce da una analisi effettuata in Inghilterra dal 2008 al 2015 dalla polizia del Durham, in collaborazione con l'Università di Cambridge, con l'obiettivo di realizzare interventi mirati a ridurre il rischio di recidiva[151]·ed è il frutto di uno studio effettuato su circa 104.000 casi avvenuti [152] , con un sistema matematico chiamato *random forest*[153](particolare forma di *machine learning)*, che prende in considerazione 34 variabili, 29 delle quali collegate alla storia criminale del soggetto, unitamente all'età, al genere, e ai codici postali di residenza[154].

Per quanto efficace, avverso tale sistema informatico sono state mosse svariate critiche da parte di chi ritiene che esso sia eccessivamente lesivo della privacy. Infatti, a supporto dell'*Hart*, si associano software come il *Mosaic code*, piattaforma informatica *Mosaic*, gestita da una compagnia privata di

[148]Cfr., OSWALD M. – GRACE J. - URWIN S. – BARNESG. C., *Algorithmic risk assessment policing models: lessons from the Durham HART model and "Experimental" proportionality*, in *Information and Communications Technology Law*, 2018, 227.
[149]Cfr., OSWALD M. – GRACE J. – URWIN S. – BARNESG. C., *Algorithmic risk assessment policing models*, cit., 227.
[150]*Ibidem.*
[151]*Ibidem.*
[152]*Ivi*, 228.
[153]*Ivi*, 227.
[154]Cfr., COUCHMANH., *Policing by Machine. Predictive Policing and the Threat to Our Rights*, in *www.libertyhumanrights.org.uk*, 2019; OSWALD M. – GRACE J. – URWIN S. – BARNESG. C., *Algorithmic risk assessment policing models*, cit., 228.

marketing, che analizza le attività personali degli individui, e l'*Experian*[155] ›un *geo-demographic segmentation tool*, che profila 50.000.000 persone in tutto il Regno Unito in 66 categorie, prendendo in considerazione oltre 850.000.000 dati, tra i più disparati, come la composizione famigliare, l'occupazione della persona, la salute, i consumi di gas ed elettricità, nonché gli *online data*[156].

È proprio l'utilizzo frequente di questi strumenti tecnologici che analizzano la sfera privata degli individui, incluse le attività telefoniche, dei *social media* e di vita sociale, in generale,[157] a sollevare le maggiori perplessità circa l'utilizzo del sistema HART[158].

4.5 Sistemi di *crime linking*

I sistemi di *crime linking* vengono utilizzati nell'individuazione delle persone per prevedere e studiare i cosiddetti reati ''a ripetizione ravvicinata'' (c.d. *near repeat crimes*) e sono riferibili a quei reati che si manifestano in un ristretto arco di tempo ed in una determinata area geografica. Esempio tipico di questi reati sono le rapine che vengono in genere ricommesse nell'arco di 48ore e, ripetute nell'arco di un mese, dagli stessi soggetti in una medesima zona come ad esempio, un determinato quartiere, una città ecc.

Il *software* raccoglie una serie di dati, come immagini di telecamere, informazioni su reati già commessi o della stessa matrice criminale, i luoghi del delitto e così via, riuscendo, così, ad individuare l'autore o gli autori della serie criminale ea prevedere la commissione di prossimi fenomeni delittuosi.

Questi *software* oltre ad essere utilizzati a fini predittivi, sono anche utilizzati, con ottimi risultati, per ricostruire la ''carriera criminale'' di un determinato soggetto e cioè avere una traccia, rilevante ai fini di indagine, che porti all'individuazione del reato commesso e di metterlo in relazione con i reati commessi dallo stesso soggetto in precedenza, se sussistenti.

---

[155]Cfr., BIG BROTHER WATCH, *Big Brother Watch's written evidence in the justice system*, cit.; ID., *A Closer Look at Experian Big Data and Artificial Intelligence in Durham Police*, 2018; ID., *Police use Experian Marketing Data for AI Custody Decisions*, 2018.
[156]Cfr., BIG BROTHER WATCH, *Big Brother Watch's written evidence in the justice system*, cit.
[157]Cfr., BIG BROTHER WATCH, *A Closer Look a tExperian Big Data and Artificial Intelligence*, cit.
[158]Cfr., GIALUZ Mitja, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *DPC-Diritto Penale Contemporaneo*, 2019, 11 s.

Vediamo adesso alcuni esempi di questa tipologia di *software*.

4.5.1 Il software *KEY CRIME*

Prima di ogni approfondimento sul software *Keycrime*, è necessario precisare, come esposto nei precedenti paragrafi, che i sistemi di polizia predittiva sono classificabili in due categorie: (i) *hotspots* (zone calde) dove il sistema analizza determinate zone dove la previsione che possano essere commessi reati è alta e dove è necessario potenziare l'attività di controllo essendo zone ad alto rischio per ciò che attiene la commissione di reati[159]; (ii) collegamenti criminali(*crime linking*) dove il sistema analizza dati relativi a crimini seriali per poter identificarne l'autore: Grazie a questo sistema, si può prevedere dove potrebbe essere commesso un reato e si può cercare di prevenirne un altro. Si può anche appurare se il reato commesso faccia parte di una serie di reati.

Keycrime appartiene alla seconda categoria ed è un *software* di intelligenza artificiale utilizzato, dal 2008, nel comune di Milano, e, dal 2009, in tutta la provincia. È stato ideato nel 2004 grazie all'intuizione di Mario Venturi un assistente capo presso la Questura di Milano che, nell'analizzare una mole di molti dati comprese che, se tutti quei dati fossero adeguatamente esaminati e incrociati fra loro, le possibilità di giungere alla soluzione del caso, in modo più efficace e più veloce, sarebbero certamente maggiori[160].

Questo sistema viene impiegato esclusivamente per i reati ''seriali'' e, si articola in due fasi: la prima individua il filo conduttore che collega la serie di

[159]Cfr., Sulle perplessità destate dall'utilizzo di strumenti di c.d. *criminal mapping* cfr. RONSIN X., LAMPOS V., MAFTREPIERREA., *Questioni specifiche della giustizia penale: prevenzione del reato, del rischio di recidiva e valutazione del livello di pericolosità, Appendice I: Studio approfondito sull'utilizzo dell'intelligenza artificiale [IA] nei sistemi giudiziari, segnatamente delle applicazioni dell'intelligenza artificiale al trattamento di decisioni e dati giudiziari*, in *www.coe.int*, 35; LUM, K. ISAAC W., *To predict and serve?*, in *Significance*, 2016, 10 vol. XIII, 14 e 19; LUM K., *Predictive Policing Reinforces Police Bias, in Human Rights Data Analysis Group*, consultabile su *www.hrdag.org*; MASSARO A., *Determinatezza della norma penale e calcolabilità giuridica*, in EDITORIALE SCIENTIFICA (a cura di), 2020, 494.

[160]Cfr., VENTURI M., KeyCrime© – *La chiave del crimine*, in *Primo Piano*, 2014, 12, 4, *www.onap-profiling.org*; MORABITO C., *La chiave del crimine*, in *www.poliziadistato.it*, 2015, 36-38; IBM in Think Milano con VENTURI Mario, *KeyCrime*, consultabile su *www.keycrime.com*, 2018.

reati; la seconda elabora i dati acquisiti per conoscere la condotta dell'autore del reato, ed è in grado di predire quando e dove verrà commesso il prossimo[161].

Keycrime è stato inizialmente impiegato per individuare gli autori (seriali) di rapine a danno di esercizi commerciali e banche (è stato, infatti, dimostrato come il 70% delle rapine di questo tipo siano riconducibili a condotte seriali[162]), ma di recente si sta sperimentando il *software* anche per i furti in appartamento[163] e, nell'immediato futuro troverà applicazione anche relativamente ad altri delitti più efferati, quali quelli di pedopornografia o, più in generale, ai reati sessuali, anch'essi, spesso, caratterizzati dalla serialità. Il software, agli inizi della sperimentazione, era in grado di immagazzinare ed elaborare fino a 11.000 *input*[164]; adesso, nella versione implementata da ''*Delia''*, le capacità di calcolo sono considerevolmente aumentate, arrivando ad incrociare fino ad 1.5 milioni di dati[165].

Keycrime attua una analisi multidisciplinare, operando in via trasversale attraverso meccanismi che appartengono a diversi settori, quali: la matematica, la statistica, la psicologia comportamentale e l'analisi geospaziale[166]. L'algoritmo è formato da dati di *input* riguardanti le caratteristiche fisiche dell'autore (corporatura, colore di capelli, età presunta, sesso, etnia, accento) e tutte le circostanze in cui si è esplicata la condotta (utilizzo di arma da fuoco, tipo di esercizio rapinato, metodo di fuga, veicolo, targa)[167].

---

[161]Cfr., VENTURI M., KeyCrime© – *La chiave del crimine*, in *Primo Piano*, 2014, 12, 4, su *www.onap-profiling.org*; MANES V., *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, cit., 6 s.; BASILE F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, cit., 12 s.; PARODI C., SELLAROLIV.,*Sistema penale e intelligenza artificiale*, cit., 56; MASTROBUONI G., *Crime isTerriblyRevealing: Information Technology and Police Productivity*, in *The Review of EconomicStudies*, vol. LXXXVII, 2020, 11, 2732.

[162]Cfr., MASTROBUONI G., *Crime is Terribly Revealing: Information Technology and Police Productivity*, cit., 2753; SABELLI C., *Scacco alla malavita: arriva l'algoritmo che prevede i reati*, in *Il Messaggero*, 2017.

[163]Cfr., Procura Generale della Repubblica presso la Corte di appello di Milano-Procura della Repubblica presso il Tribunale di Milano, *Bilancio di responsabilità sociale 2018*, www.ca.milano.giustizia.it.

[164]Cfr., VENTURI M., KeyCrime© – *La chiave del crimine*, cit. 5; MASTROBUONI G., *Crime isTerriblyRevealing: Information Technology and Police Productivity*, cit., 2741; SCOVACRICCHI C., *Quando il poliziotto diventa startupper. La storia di* Keycrime, in www.startupmagazine.it, 2018.

[165]Cfr., *www.keycrime.com.*

[166]Cfr., VENTURI M., KeyCrime© – *La chiave del crimine*, cit. 5 s.

[167]Cfr., MASTROBUONI G., *Crime is Terribly Revealing: Information Technology and Police Productivity*, cit., 2741; ID. (Lead Academic) *Impact: Imagine being able to predict a crime in the future, Research case study by University of Essex*, in *www.essex.ac.uk*; MORABITO C., *La chiave del crimine*, cit., 2015, 36 e 38.

Tutti questi dati vengono raccolti attraverso prove documentali e testimoniali o attraverso immagini per essere, poi, trasferiti nel *software* che ricerca elementi di contatto rispetto ad altri contenuti nel *dataset***.** Dall'*input*, rappresentato dai dati raccolti e correlati ai dati contenuti nel database *Keycrime*, si ottiene l'*output* cioè il risultato elaborato dal sistema informatico che consente il collegamento fra reati, individuando la serie criminosa ascrivibile al medesimo autore e permettendo di prevedere il dove, come e quando, potrebbe verificarsi il prossimo reato[168].

In sintesi, nella prima fase, mediante una analisi induttiva, vengono confrontati ed analizzati i dati presenti nel *software* al fine di individuare le caratteristiche proprie dei reati seriali[169]; nella seconda fase, mediante una analisi deduttiva, è possibile comprendere le modalità di azione dell'autore e di prevedere dove, quando e come, il nuovo crimine avrà luogo[170].

Keycrime, come dimostrano i tassi di successo, si è rivelato un applicativo molto utile ed efficace.

Ai fini di una giusta comprensione del procedimento investigativo, risulta necessario chiarire una questione rilevante: la distinzione tra la polizia di prevenzione e quella giudiziaria. Le due forze di polizia differiscono per il fatto che una svolge attività di prevenzione dei reati, mentre l'altra svolge funzione repressiva in stretto contatto con gli Uffici delle Procure della Repubblica. Compito della polizia giudiziaria è quello di raccolta delle prove, finalizzata alla individuazione del reo; compito della polizia di prevenzione è quello di prevenire o ridurre gli eventi criminosi [171], proprio per questo, è un'attività è finalizzata a garantire l'ordine pubblico e la sicurezza.

---

[168]Cfr., MORABITO C., *La chiave del crimine*, cit., 2015, 36 e 38; PELLICCIA R., *Polizia Predittiva: il futuro della prevenzione criminale?*, cit.: «Lo studio [dell'Università di Essex] ha evidenziato un consistente punto di forza di *Keycrime* rispetto ai competitor. Mentre questi lavorano su base puramente statistica, indicando dove, quando e che tipo di crimine sarà commesso, *Keycrime* si offre di definire anche il come, grazie a un'analisi delle modalità comportamentali dell'autore, ai suoi tratti psicologici.».

[169]Cfr., VENTURI M., KeyCrime© – *La chiave del crimine*, cit. 5 s.

[170]Cfr., VENTURI M., KeyCrime© – *La chiave del crimine*, cit. 6.

[171]Cfr., Ai sensi dell'art. 1 del R.D. 18 giugno 1931, n. 773 (Testo unico delle leggi di pubblica sicurezza) l'autorità di P.S. "«veglia al mantenimento dell'ordine pubblico, alla sicurezza dei cittadini, alla loro incolumità e alla tutela della proprietà; cura l'osservanza delle leggi e dei regolamenti generali e speciali dello Stato,delle province e dei comuni, nonché delle ordinanze delle

Mentre la polizia giudiziaria svolge indagini, volte alla acquisizione delle prove, dopo la commissione del crimine, la polizia preventiva, svolge ricerche circa i dati relativi ad individui che si ritiene siano sul punto di commettere dei reati.

In Italia la polizia preventiva si avvale di *Keycrime*, che ha una doppia finalità sia di prevenzione (quindi ante-reato), sia investigativa (dopo il reato).

Se il software *Keycrime*, è uno strumento utilissimo per prevenire reati seriali, è pur vero che, avvalendosi di dati online, si può incorrere in errore, nella violazione della privacy dei cittadini e in effetti discriminatori. Infatti, si è evidenziato che porre l'attenzione su un soggetto come possibile autore di un reato, al posto di altri, con medesime probabilità di essere autori di futuri reati, sia un elemento potenzialmente discriminatorio, anche nel caso in cui, in un secondo momento, la previsione algoritmica risultasse veritiera.

Per ciò che attiene la ricostruzione degli eventi passati che sono utili per ricostruire una serie di elementi ''pericolosi'' riconducibili ad un medesimo soggetto, è indispensabile che queste informazioni, per usufruirne in sede dibattimentale, siano state acquisite nel rispetto delle norme codicistiche; diversamente si incorrerà nel "divieto di utilizzabilità" espressamente sancito dall'art. 191 c.p.p. Per lo stesso motivo, immagini particolari, indumenti indossati dall'autore del reato in varie occasioni, per essere considerate prove ammissibili devono essere mostrate precedentemente al Tribunale ("ostensione"). Stesso discorso vale per le dichiarazioni raccolte, in sede investigativa, che devono essere supportate da una successiva testimonianza. Solo in presenza di tutti questi elementi, i dati possono essere presi in considerazione in sede dibattimentale.

5. Il tema delle indagini in tempo reale

Coerentemente a quanto è stato discusso nel precedente capitolo[172], i *broker* privati raccolgono miliardi di dati personali, comprese indicazioni sulla vita individui e sulla loro sfera privata come l'abitazione e la famiglia. La

autorità; presta soccorso nel caso di pubblici e privati infortuni"; "per mezzo dei suoi ufficiali, e a richiesta delle parti, provvede alla bonaria composizione dei dissidi privati".

[172] V. paragrafo 1, Capitolo I.

polizia predittiva, tramite la tecnologia dei *big data*, può, quindi, venire a conoscenza di informazioni rilevanti, prima di agire contro determinati soggetti. Le forze dell'ordine di Fresno, in California, hanno pilotato un progetto volto a testare il funzionamento del servizio c.d. *Beware*; questo per fornire alle aziende private di dati, informazioni in tempo reale sull'indirizzo delle persone che hanno effettuato una chiamata al 911.Questi *data* vengono poi suddivisi e classificati come *''threat score''* (punteggi di portata)[173].Questa operazione è stata fatta con uno scopo: usufruire delle grandi banche dati, che analizzano i consumatori, per effettuare, anticipatamente, un giudizio predittivo circa le caratteristiche del chiamante e/o del quartiere in cui abita (se rischioso o meno)[174]. Le previsioni *Beware* vengono effettuate attraverso livelli di minaccia codificati e suddivisi in base ai colori (*color-coded*), rosso, giallo, e verde, e fornivano, così, una determinata misura di valutazione del rischio per la polizia. Il problema dell'algoritmo *Beware* è che non sono note le modalità, alla base del suo funzionamento, mediante le quali riesce a determinare il livello di rischio, creando così problemi di trasparenza. Intrado, infatti, filiale di West Corporation, nonché azienda proprietaria di *Beware*, ha mantenuto segreto il linguaggio di programmazione del software per nasconderlo al mercato[175]. Addirittura, in base a quanto affermato dal capo della polizia di Fresno, Intrado non aveva nemmeno informato le forze dell'ordine circa il *modus operandi* utilizzato per il calcolo dei punteggi di rischio. Permane, altresì, come ulteriore questione, la possibilità che i dati, utilizzati per l'indagine circa la minaccia di criminalità, siano errati, con il conseguente rischio di inficiare tutto il processo conoscitivo algoritmico. A New York, invece, è stato spesso utilizzato, per le indagini in tempo reale, il *Domain Awareness System* (*DAS*), un software nato dalla *partnership* tra la polizia di New York e Microsoft. Il *DAS* è in grado di collegare circa novemila telecamere di sorveglianza a circuito chiuso per favorire il monitoraggio in

[173]Cfr., 1. JUVENAL Justin, *The New Way Police Are Surveilling You: Calculating Your Threa t*"Score," in *Wash. Post*, 2016.
[174]*Ibidem.*
[175]Cfr. ROBINSON David, *Buyer Beware A tard Look at Police "Threat Scores"*, v. TURE, 2016, available at *www.equalfuture.us*.

real-time di Manhattan[176]. I video rilevati sono collegati direttamente ad un sistema di allarme digitale che traccia automaticamente i comportamenti sospetti, come ad esempio lasciare una borsa in strada e poi allontanarsi. Le telecamere raccolgono, altresì, le immagini delle auto e delle targhe, tracciando, così, tutte le vetture che transitano in una determinata area. I lettori di rilevazione delle targhe (gli *ALPRs*) sono collegati, a loro volta, ai c.d. registri *DMV*[177], alle liste di controllo del rischio della polizia, ai mandati, ai database terroristici, e a tutte le informazioni personali sospette associate a questi database[178](es. si rileva mediante le telecamere il profilo di un individuo segnalato come pericoloso o ricercato). Il video registrato dalle telecamere può essere anche riprodotto in un secondo momento per tracciare la direzione, la posizione, gli spostamenti o movimenti di un sospettato. La tecnologia, dopo aver tracciato un profilo del soggetto pericoloso o rischioso, può persino cercare e confrontare nella città soggetti con caratteristiche simili tramite le videocamere disseminate in tutte le aree urbane, segnalando alla polizia ad esempio: ''Si ricerca un soggetto con indosso una camicia rossa, vicino la Borsa di New York''[179].Possono essere isolate alcuni *frame* di immagine dai video, contrassegnati per posizione, data e ora, e confrontati con i volti dei sospettati. Tramite questi strumenti di tracciamento, il *DAS* è in grado di seguire il percorso di un soggetto segnalato, grazie all'ausilio delle telecamere, fino a trovarlo, e tramite la targa di un'auto può risalire al proprietario e scoprire se è stata rubata o meno. Allo stesso modo l'auto di fuga potrebbe essere rintracciata e analizzata.

Per aumentare ulteriormente la condivisione dei dati l'*NYPD* ha investito in tremilacinquecento *smartphones* in modo che gli agenti di pattuglia potessero sempre avere aggiornamenti dal programma *DAS*, in tempo reale, sul controllo cittadino e sulla eventuale criminalità[180].

---

[176]Cfr., DAVENPORT Thomas H., *How Big Data Is Helping the NYPD Solve Crimes Faster*, in *Fortune*, 2016.
[177] V., *https://dmv.ny.gov/driver-license/online-vision-registry.*
[178]*Ibidem.*
[179]Cfr., MANHUNT--*Boston Bombers*, in NOVA (a cura di), 2013, *www.youtube.com/watch?v=ozUHOHAAhzg.*
[180]Cfr., FLEISCHER Tim, *Officers Embrace New Smartphones as Crime Fighting Tools*, in *ABC7NY*, 2015, *http://abczny.com.*

Simili al sistema di sorveglianza di New York, in altre città, quali ad esempio, Los Angeles e Fresno, sono state testati in versione ridotta, cioè utilizzando meno telecamere e in aree più piccole[181].È chiaro che, grazie all'ausilio di questi nuovi meccanismi investigativi, la possibilità di prevenire il crimine, in modo più efficace, è maggiore rispetto alle indagini definibili come ''tradizionali''.

Le tecnologie digitali *all-seeing*, quindi, se da una parte aumentano le capacità investigative del sistema giudiziario, dall'altra accelerano, altresì, i tempi di reazione della polizia. La sorveglianza in tempo reale può fornire una vasta gamma di informazioni utili alla polizia come ad esempio: chi si trova sulla scena del crimine, (elemento in genere difficile da provare a mezzo delle indagini ''ordinarie''), risalire all'iter storico del fatto criminoso, o, in generale, cercare, con più facilità, gli individui pericolosi. L'ausilio del sistema *real-time* può essere davvero di aiuto anche quando è necessario inviare servizi medici di primo soccorso per emergenze, accorciando il periodo di arrivo dell'ambulanza, in situazioni in cui spesso anche pochi minuti di ritardo possono essere vitali. Il tempo di risposta dei servizi in generale, quindi, migliora grazie all'automazione, con l'uso di algoritmi che utilizzano le telecamere cittadine come vere e proprie ''spie digitali'', in grado di riconoscere modelli sospetti e avvisare la polizia[182].

A East Orange, nel New Jersey, la polizia ha adottato i c.d. *Avista Smart Sensors di Digisensory Technologies* per monitorare automaticamente le strade[183]. Queste telecamere intelligenti sono state addestrate per cercare modelli di attività sospette, elaborando 60 miliardi di istruzioni al secondo[184]. Per esempio, ripetute e frequenti transazioni *hand-to-hand* in un angolo possono tradursi in fattispecie criminose di spaccio, o ancora un rapido

[181]Cfr., JOUVENAL Justin, T*he New Way Police Are Surveilling You: Calculating Your Threat "Score"*, in *Wash. post*, 2016.
[182]Cfr., RICH Michael L., *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment,* in *U. Pa*, 2016, 871-880,164.
[183]Cfr., AOL Digital Justice, *Digisensory Technologies Avista Smart Sensors*, 2012, available at *www.youtube.com/watch?v=JamGobiSswg*; Associated Press, NJ City Leading Way in Crime-Fighting Tech, in *CBSNEWS*, 2010, *www.cbsnews.com*.
[184]Cfr., BONDY Halley, *East Orange Installs Surveillance Cameras That Sense Criminal Activities, Alerts Police*, in *Star- Ledger*, Newark, 2010, *www.nj.com*.

movimento verso una persona e poi scappare potrebbe indicare una rapina o un furto. I sensori monitorano le azioni sulla strada e avvisano immediatamente la polizia se la scena osservata corrisponde a un modello che il sensore è stato addestrato a identificare come pericoloso. Una volta che il sensore si attiva, gli agenti più vicini vengono automaticamente avvisati del potenziale crimine, dell'ora e della posizione. Le telecamere possono rintracciare la scena, e, dal quartier generale, sessanta comandanti possono assicurarsi che l'algoritmo abbia previsto una giusta intuizione, onde evitare errori.

Esistono algoritmi simili, programmati allo scopo di identificare i colpi di pistola mediante sensori audio. Si tratta della tecnologia c.d. *Shot Spotter* che fornisce rapporti automatizzati sui *''gunshots''* in grado di informare la polizia prima di eventuali testimoni oculari, accelerando il processo investigativo[185].Non appena il microtono altamente sensibile riconosce il suono dell'arma da fuoco, la polizia viene immediatamente avvertita in modo da potersi dirigere verso il *locus* criminoso. I veicoli si trovano più velocemente, i colpevoli catturati e i testimoni intervisto. Questi sensori automatici sono stati installati a Washington, D.C., a Boston, a Oakland, a San Francisco e a Minneapolis[186].

La tecnologia del *real-time* mostra una velocità di risposta al crimine incomparabile rispetto alla risposta umana.

Come accennato in precedenza, nel presente paragrafo, un altro sistema in tempo reale davvero efficace è quello dei lettori di targhe i c.d. *ALPRs*. Questi dispositivi sono simili alle videocamere di sorveglianza e riescono a scansionare una targa e confrontare automaticamente le informazioni del proprietario, la patente o altre licenze associate all'auto, con i database contenenti mandati, auto rubate, caselli autostradali non pagati e altre variabili valutate caso per caso[187].

[185]Cfr., WATTERS Ethan, *ShotSpotter*, in W*ired,* 2007, 146 e 152; NEAGLE Colin, *How the Internet of Things Is Transforming Law Enforcement*, in *Network World*, 2014.
[186]Cfr., SCHLOSSBERG MARCH Tatiana, *New York Police Begin Using ShotSpotter System to Detect Gunshots*, in *N.Y. Times*, 2015.
[187]Cfr., MEROLA Linda &LUM Cynthia, *Emerging Surveillance Technologies: Privacy and the Case of License Plate Recognition* (*LPR) Technology*, in *JUDICATURE* 96:3 119-21, 2012.

I sistemi *ALPRs* sono in grado di scansionare migliaia di targhe al giorno. In pratica, un agente di polizia guidando sull'autostrada, può notare un'auto sospetta e ottenere riscontro in tempo reale dal database del programma, per esempio, per scoprire se il veicolo rientra tra quelli rubati[188].

Abbastanza sofisticati da rilevare circa una targa al secondo, l'algoritmo *ALPR* può generare mappe *ad hoc* indicanti la posizione, in tempo reale, delle auto, tracciando persino il percorso per raggiungerle. Una mappa *ALPR* può, quindi, collegare auto e proprietari per ora, data e posizione. I dati sul tracciamento delle auto, protratto nel tempo, forniscono indizi sulle abitudini del proprietario quali i modelli di viaggio e la posizione effettiva delle auto in determinati momenti del giorno, del mese o dell'anno[189].

Si pensi al caso in cui la polizia sospetti attività di spaccio di droga in una particolare abitazione, l'avvistamento ripetuto di una targa, in quel luogo, potrebbe fondare un indizio concreto per la conferma del suddetto sospetto. L'algoritmo *ALPRs* può essere di grande aiuto anche in situazioni di salvataggio di emergenza, come nel caso di rapimento di bambini, segnalato dal software *"Amber Alert"*[190].

Un tale database di informazioni GPS, che si fonda su un continuo tracciamento, naturalmente, presenta un grave problema di lesione della privacy, dato che tutti gli individui, proprietari di un'auto possono essere potenzialmente risucchiati nel flusso di indagine su larga scala, rendendo così pressoché pubbliche tutte le attività personali[191].

Le telecamere di sorveglianza avanzate a Los Angeles, addirittura, hanno la capacità di scansionare e confrontare le immagini facciali, registrate nelle strade ogni giorno, con chiunque sia presente, come sospettato, nel database della polizia. Con lo stesso meccanismo usato per risalire ad un'auto con una

[188]Cfr., RUSHIN Stephen, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH.& POL'Y 281, 285-86.
[189]Cfr., KAMINSKI Margot E., *Regulating Real- World Surveillance*, in *Wash.*, 2015, 1113 -1153, 90.
[190]Cfr., MARTINEZ Michael, *Policing Advocates Defend Use of High-Tech License Plate Readers*, in *CNN*, 2013, *www.cnn.com*.
[191]Cfr., WILSON Simone, *L.A. Sheriff's Creepy New Facial-Recognition Software Matches Surveillance Video with Mug Shot Database*, in *L.A. wkly*., 2012.

targa, una persona ricercata per una attività criminale può essere identificata automaticamente utilizzando le tecnologie di riconoscimento facciale[192].

In aggiunta, una mappa digitale degli avvistamenti passati è accessibile alla polizia, dal programma, per un uso investigativo successivo, in modo che, se un crimine si è verificato vicino a una telecamera, la polizia può scorrere indietro fino a giungere al momento focale del video e identificare tutte le persone che sono passate davanti alla telecamera nel tempo pertinente al fenomeno delittuoso.

Simile al funzionamento del *Domain Awareness System*, la polizia può ripristinare il nastro e studiare come si è sviluppato il crimine, dove sono fuggiti i colpevoli e i modelli comportamentali antecedenti e successivi alla commissione del crimine.

La tecnologia di riconoscimento facciale associa le impronte digitali virtuali a chiunque si trovi davanti a una telecamera. L'*FBI* possiede un database di circa 30 milioni di fotografie e, così, anche di impronte [193]

Alcune fotografie provengono da foto della patente di guida, il che significa che milioni di persone innocenti vengono regolarmente registrate insieme alle foto dei criminali[194], molte altre derivano da arresti penali. In poco meno di cinque anni, l'*FBI* ha richiesto 215.000 ricerche nei database di riconoscimento facciale, con 36.000 indagini nei database di patenti di guida statali[195].

Se collegato con funzionalità video in tempo reale e sofisticate tecnologie di riconoscimento facciale, una nuova rete di sorveglianza visiva potrebbe presto diffondersi nelle città.

La crescita dell'uso delle telecamere per l'individuazione del ''corpo'' (*police-worn body*) indossate dalla polizia fornisce ulteriori capacità di

---

[192]Cfr., FERGUSON, A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, in *NYU Press,* 2017, 89, *https://doi.org/10.2307/j.ctt1pwtb27.4.*

[193]Cfr., *General Accounting Office face recognition technology, fbi should better ensure privacy and accuracy* 10 (*report to the Ranking Member, Subcommittee on Privacy. Technology and the Law; Committee on the Judiciary, U.S. Senate*, 2016).

[194]Cfr., GARVIE Clare, BEDOYA Alvaro, & FRANKLE Jonathan, , *The perpetual line- up: unregulated police facial recognition in america* in *Georgetown Law Center on Privacy & Tech* 2016), available at *www.perpetuallineup.org*.

[195]*Ivi,* 17.

identificazione. Le *police-worn body cameras* (perché appunto indossate dalla polizia) sono piccole telecamere apposte di solito sulla parte anteriore di un'uniforme, e alcuni dipartimenti di polizia hanno persino adottato un software che consente agli *smartphones* di aumentare le potenzialità delle telecamere da remoto[196].Queste telecamere creano un *feed* (valutazione) continuo sulle persone con cui la polizia entra in contatto durante le operazioni di routine quotidiana[197]. Il video può essere utilizzato per identificare chi, dove e quando ha preso contatto la polizia. Le telecamere per il corpo di nuova generazione includeranno una tecnologia di riconoscimento facciale in tempo reale che consentirà alla polizia di conoscere mandati attivi, violenze precedenti o comportamenti innocui[198].

Inoltre, la stessa tecnologia di riconoscimento facciale sta diventando più sofisticata di mese in mese.

Se il *DAS* e le telecamere del corpo non lo sono abbastanza, la telecamera real-time aeree, fornisce l'ultimo strumento di *survellance* di massa senza precedenti.

Volando in alto sulle città, e in grado di registrare l'attività di interi quartieri, per ore, le telecamere aeree, come *Persistent Surveillance Systems* possono controllare il crimine in tempo reale e segnalare i modelli di tutti i veicoli coinvolti, le persone e gli eventi pertinenti[199].

Se si aggiungessero, a questi sistemi avanzati, sofisticati sensori audio, la sorveglianza sarebbe senza precedenti a 360 gradi, nulla più sfuggirebbe alla polizia, avendo controllo in ogni momento, di qualsiasi attività cittadina. Gli aerei dei sistemi di sorveglianza persistenti hanno volato in missioni su Baltimora, Los Angeles, Indianapolis, Charlotte e altre città[200]. Con questi appositi meccanismi, il tempo e il movimento possono essere ridotti a geo-dati

---

[196]Cfr., FARIVAR Cyrus, *Meet Visual Labs, a Body Camera Startup That Does it Sell Body Cameras*, in *Arstechnica*, 2016, *http://arstechnica.com*.
[197]Cfr., JOH Elizabeth E., T*he New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, in *Harv. L. & Pol'Y*, 2016, 15, 10.
[198]Cfr., WEISE Karen, *Will a Camera on Every Cop Make Everyone Safer? Taser Thinks So*, in *Bloomberg business week*, 2016.
[199]Cfr., REEL Monte, *Secret Cameras Record Baltimore's Every Move from Above*, in *Bloomberg business week*, 2016.
[200]*Ibidem.*

ricercabili in appositi *database*. Una storia digitalizzata permette di riconquistare il normale passaggio del tempo.

Questi nuovi sistemi di sorveglianza sono stati testati in missioni a Baltimora, Los Angeles, Indianapolis, Charlotte e altre città[201]. Questo potrebbe essere il futuro delle indagini.

La più antica tradizione investigativa in materia di sospetto di omicidio sostiene che le prime 48 ore di indagine sono le più importanti, a volte persino vitali. L'uso dei nuovi algoritmi predittivi, sistemi di sorveglianza, analisi e confronto dei *big data* potrebbero essere di grande aiuto per rendere le indagini più veloci.

Sarah Brayne ha condotto un innovativo studio di due anni e mezzo sull'adozione della tecnologia basata sui dati da parte della polizia di Los Angeles[202]. Brayne descrive come i grandi set di dati abbiano reso le indagini della polizia più veloci, accurate[203]. La ricerca si basa su un'indagine per omicidio iniziata con il ritrovamento di un corpo rinvenuto in una località remota. La vittima sembrava essere un membro della banda di Los Angeles, ma non è stato possibile individuare alcun testimone. Fortunatamente, uno scanner automatico di targhe ha registrato le auto vicine al *locus commissi delicti*. Analizzando i video di sorveglianza e isolando l'ora del giorno, in cui presumibilmente il crimine si era verificato, la polizia si è concentrata su una singola targa rilevata più volte, dal sistema *ALPRs*, a Compton, in California. Successivamente, incrociando il nome del proprietario con un database di bande, la polizia ha identificato un individuo, facente parte di una banda rivale della persona uccisa. Il veicolo del sospetto è stato perquisito e sono state recuperate prove incriminanti che collegavano il soggetto alla vittima[204], così il caso è stato risolto con modalità assai veloci ed efficaci.

I sistemi, di analisi e confronto di dati, consentono, quindi, alla polizia, di elaborare più informazioni in modo più rapido.

---

[201] *Ibidem.*
[202] Cfr., BRAYNE Sarah, *Stratified Surveillance: Policing in the Age of Big Data*, 9 e 13.
[203] *Ibidem.*
[204] *Ivi*, 23 s.

Palantir ha sviluppato un sistema di analisi dati che consente alla polizia di cercare, in appositi database, dati su: persone, automobili, case, telefoni cellulari, indirizzi e-mail, luoghi, amici, associati/affiliati, familiari e occupazione, nonché informazioni provenienti da servizi sociali, servizi sanitari, servizi di salute mentale, pignoramenti, social media, bollette, persino registrazioni telefoniche memorizzate [205]e mapparli digitalmente. Questo permette alla polizia di conoscere la natura delle reti criminali nelle città e tentare di bloccarle[206]. Un tale sistema di aggregazione di dati, tuttavia, potrebbe causare problemi di privacy, ancor di più quando si tratta di analizzare informazioni sensibili (es. sanitarie).

Questi *thread* di collegamenti, con l'ausilio di appositi sistemi come *''geofence''*, un sensore elettronico che avvisa la polizia quando qualcuno attraversa una determinata area ''rischiosa'', possono creare un vero e proprio screening sulla delinquenza cittadina, tracciando dati e movimenti criminali[207], in modo tale, ad esempio, che se una singola auto attraversa ripetutamente quelle zone segnalate, si può dedurre che gli individui nella vettura siano coinvolti nella sospetta attività illecita. Tutto queste operazioni possono essere effettuate in tempo reale (*real-time*). Invece di condurre un c.d.''*stake-out''*, è possibile creare un sistema di allarme automatico volto a segnalare agli ufficiali di polizia che una particolare auto è entrata in un'area segnalata, associando al fenomeno eventuali chiamate alla polizia oppure la rilevazione del sensore di un particolare soggetto rischioso. Il sistema funziona così: ogni volta che una persona ricercata entra in contatto con il sensore (attraversando l'area in cui è riposto), l'ufficiale di polizia riceve un'e-mail che lo informa dell'accaduto, in modo che possano essere inviate delle pattuglie sul posto. Inoltre, simile a quanto accade con il sistema *Beware*, tutti questi sistemi legati alla tracciabilità del *locus* criminoso possono indicare agli agenti dove dirigersi, dopo la risposta ad una chiamata di emergenza o prima di effettuare un arresto. I dati sulla zona,

[205]Cfr., PATTERSON Thom, *Data Surveillance Centers: Crime Fighters or "Spy Machines*"?, in *CNN* , 2014, available at *www.cnn.com.*
[206]*Ibidem.*
[207]Cfr., HACKETT Chris & GROSINGER Michael, *The Growth of Geofence Tools within the Mapping. Technology Sphere,* in *Pdv wireless*, 2014, *www.pdvwireless.com.*

l'indirizzo, i crimini passati nel quartiere e altri dati, che sono stati inseriti in precedenza nel sistema, possono essere forniti a necessità dell'agente in maniera quasi istantanea. L'automazione spinge, così, ogni giorno di più, le strategie tattiche della polizia ad un livello superiore sul punto di vista dell'accuratezza ed efficacia investigativa.

6. Le opportunità e le criticità della polizia predittiva

È stato descritto, nei precedenti paragrafi, come la polizia preventiva si attesti a diventare un perno centrale nella fase delle indagini e, in generale, nella giustizia penale in quanto il suo scopo è quello di tutelare la sicurezza del singolo e della collettività e di individuare i crimini futuri al fine di prevenirli. Tuttavia, sono ancora molte le questioni problematiche. Si assiste, infatti, giorno per giorno, ad una continua evoluzione dell'intelligenza artificiale che rende impossibile prevederne gli sviluppi futuri[208]. Occorre che tale tecnologia venga applicata in modo controllato per evitare disfunzioni del sistema. Nonostante le varie criticità l'IA può essere un importante strumento ad ausilio delle attività giudiziarie in quanto, spesso, l'essere umano può commettere errori.

In primis è importante porre l'attenzione sulle metodologie euristiche adottate dagli operatori giudiziari nell'espletamento delle loro funzioni legate alla prevenzione o repressione della criminalità. Ciò è importante perché, anche se i procedimenti penali si svolgono in un'ottica di imparzialità ed oggettività della giustizia, è pur vero che la stessa obiettività può essere contaminata da influenze esterne, come fattori psicologici personali che possono condizionare la conduzione delle indagini e che nulla hanno a che vedere con un reato compiuto o che si prevede possa essere commesso. L'influenza dei fattori

[208]Cfr., Per approfondire il tema dell'intelligenza artificiale come fine ultimo del diritto penale, v. C. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen.*, 2019, 1908 ss., 4: «gli algoritmi intelligenti sono in grado attraverso la tecnologia di affrontare, a vantaggio di tutti, problemi quotidiani che, tuttavia, vanno oltre le capacità umane; e certamente meglio, più velocemente e in modo più economico rispetto ai decisori umani». Cfr. altresì MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia, in Intelligenza artificiale*. Il diritto, i diritti, l'etica, in RUFFOLO U. (a cura di), 2020, 547 ss.

''umani'' come le condizioni mentali ed ambientali modifica enormemente l'attività cognitiva e decisiva, tanto da "deviare'' il c.d. ragionamento corretto. Le caratteristiche psicologiche svelano quanto i meccanismi basali della nostra vita (anche riguardanti le più banali attività quotidiane) mutino costantemente, in relazione all'umore, agli accadimenti giornalieri ecc., al punto da inficiare il c.d. ragionamento corretto.

Sintomatico è un esperimento fatto su otto giudici israeliani[209]che, per dieci mesi, sono stati esaminati in dieci sedute giornaliere. Le giornate venivano ripartite in tre fasce lavorative ed i giudici erano chiamati a decidere sulle richieste di libertà condizionale a favore di vari detenuti. Lo studio ha dimostrato che nella prima fascia mattutina venivano concesse più volte, fino a diminuire quasi a zero nella fascia pomeridiana. Lo studio ha dimostrato, quindi che fattori come il passare del tempo, la pausa di lavoro, la stanchezza, la fame, la noia, ed altro, sono fattori di rischio che incidono sulla decisione[210]. Molti sono gli studi effettuati in tale senso e, tutti hanno condotto a questa conclusione e, cioè che circostanze esterne possono influenzare il giudicato[211].

È proprio per evitare questo fenomeno che viene utilizzata l'IA, per eliminare, quanto più possibile i pregiudizi (*bias*) che pervadono i procedimenti penali[212]. In quest'ottica, l'IA assume un ruolo preminente e, per questo, è al centro del dibattito giuridico[213]. Grazie ad essa vengono raccolti innumerevoli

---

[209]Cfr., Lo studio è riportato sinteticamente nell'introduzione di un contributo sul ragionamento dei giudici, realizzato da logici e filosofi della scienza. Lo studio originale, invece, è da attribuire a «DANZIGER, LEVAV e AVNAIM-PESSO, 2011, ripreso poi da moltissimi altri, compreso KAHNEMAN (2011, 48 e 9), che ne ha curato la pubblicazione su *PNAS* (la prestigiosa rivista della *National Academy of Science* americana). L'interpretazione più comune, suggerita anche dagli autori, è che il deperimento progressivo delle risorse cognitive dei giudici determini una tendenza a scegliere l'opzione "di default", cioè a favore dello status quo. Commenti critici rilevanti sui dettagli dello studio e soprattutto sulla sua interpretazione sono in WEINSHALL-MARGEL e SHAPARD, 2011 e GLÖCKNER, 2016». Cfr. CEVOLANI G. – CRUPI V., *Come ragionano i giudici: razionalità, euristiche e illusioni cognitive, in Criminalia*, 2017, 181 ss.

[210]*Ibidem.*

[211]Cfr., ENGLICH B.– MUSSWEILER T. – STRACK F., *Playing Dice With Criminal Sentences: The Influence of Irrelevant Anchors on Experts' Judicial Decision Making, in Personality and Social Psychology Bulletin*, 2006, 4, 194.

[212]Cfr., Sul problema dei pregiudizi (*bias*), v. *amplius* DI GIOVINE O., *Il judge-bot e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale*), in Cass. pen., 2020, 3, 951 ss.

[213]Cfr., Sul punto, v. Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, adottata dalla Commissione europea per l'efficacia della giustizia (CEPEJ) nel corso della sua 31° Riunione plenaria, Strasburgo, 3-4 dicembre 2018, 35, § 7: «Gli strumenti denominati di "polizia predittiva" (prima del processo giudiziario o del rinvio a giudizio)

quantità di dati che successivamente vengono elaborati e "ripuliti" da elementi di parzialità. Questi nuovi algoritmi, per evitare il problema di dati fuorvianti, funzionano solo quando dai dati deriva un input, segnalato dal software come di ''qualità'', e corrispondente alla realtà fattuale, tramite la tecnologia del *matching*.

Per una maggiore efficacia della procedura di elaborazione algoritmica è opportuno sottoporre all'analisi soltanto un *numerus clausus* di variabili di dati, quelle cioè indispensabili per una valutazione oggettiva, trasparente e imparziale del caso in esame. È evidente che l'analisi algoritmica di partenza può essere successivamente ampliata con l'aggiunta di altri dati che completino il quadro conoscitivo con particolari del caso e circostanze non esaminati in precedenza. In questo modo, incrementando il *data collection*, l'algoritmo è in grado di migliorare il proprio apprendimento automatico, elaborando valutazioni sempre più precise e attendibili.

Un'altra criticità relativa alla raccolta dei dati è rappresentata dalla loro *quantità*, ad esempio a seconda che si operi in grandi o piccole città o in aree geografiche medie o grandi, dato che è un fattore che condiziona l'efficienza del funzionamento dell'algoritmo.

L'utilizzo dei dati lede enormemente la *privacy* e la proprietà. Ciò trae origine dal fatto che il quotidiano scambio di dati informatici a livello nazionale

---

sono già in rapida crescita e cominciano a essere noti al grande pubblico (si pensi per esempio alla lista di interdizione al volo [*no fly list*], che è in realtà un'applicazione dell'analisi dei megadati, che raccoglie e analizza dati riguardanti potenziali terroristi al fine di prevenire la commissione di atti, o agli algoritmi utilizzati per scoprire le frodi o il riciclaggio di denaro). In generale, si utilizzano correntemente un gran numero di strumenti informatici per prevenire la commissione di reati (mediante l'individuazione dei possibili luoghi in cui ciò potrebbe avvenire o i loro autori) o per perseguirli in maniera più efficace. La prima categoria comprende gli strumenti di "polizia predittiva" utilizzati per prevenire alcune tipologie di reato la cui commissione presenta elementi di regolarità, quali il furto con effrazione, la violenza di strada, il furto di veicoli o di oggetti situati al loro interno. La designazione di tali strumenti deriva dalla loro capacità di determinare con precisione dove e quando potrebbero essere commessi tali reati e di riprodurre tali informazioni su una carta geografica sotto forma di "punti caldi" sorvegliati in tempo reale da pattuglie della polizia. Tale processo è denominato "mappatura dei rischi di reato" [*predictive criminal mapping*]. La maggior parte dei software utilizzati in tale ambito si fondano su elementi di localizzazione storica dei reati forniti dai rapporti di polizia, ma sono in fase di sperimentazione nuove tecnologie ancora più potenti che combinano vari dati provenienti da fonti differenti. Tali strumenti, che hanno tassi di efficacia molto convincenti, hanno assertivamente anche effetti dissuasivi in ordine alla commissione di reati nelle zone circostanti i punti segnalati, il che conduce a un'opinione positiva delle politiche pubbliche».

ed internazionale, attraverso la modalità *remote-controlled* viola ripetutamente la riservatezza degli utenti senza limiti territoriali.

A protezione della *privacy* e dei dati personali degli individui nelle attività di polizia e giudiziarie (in particolare delle persone coinvolte in procedimenti penali, che siano testimoni, vittime o indiziati) è intervenuta, sul tema, la Direttiva 2016/680 (in aggiunta al Regolamento Generale sulla Protezione dei Dati—GDPR 2016/679 e al Regolamento UE 2018/1725 sulla tutela delle persone fisiche, in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli organismi dell'Unione) che stabilisce un quadro normativo *ad hoc*, limitando l'uso sproporzionato ed eccessivamente invasivo delle informazioni. Tale Direttiva contribuisce a facilitare la cooperazione tra Stati contro la criminalità in Europa, armonizzando la disciplina della protezione dei dati personali. I punti chiave della normativa garantiscono che i dati raccolti dalle autorità incaricate: i) siano trattati in modo lecito e corretto; ii) siano elaborati per finalità esplicite (c.d. obblighi di trasparenza) e legittime; iii) siano pertinenti e non eccedenti rispetto alle finalità per le quali erano stati raccolti; iv) siano esatti (ossia veritieri) e aggiornati; v) siano adeguatamente protetti, onde evitare abusi di trattamento e lesione della riservatezza.

Nel giugno del 2023, inoltre, il Parlamento UE ha tentato di regolamentare la disciplina dell'IA in un unico testo normativo, attualmente ancora in fase di negoziazione (*AI ACT*), che introduce nuove e innovative regole, volte a garantire sicurezza, affidabilità ed etica dei sistemi di Intelligenza Artificiale all'interno dell'Unione Europea. In particolare, è stato vietato: i) l'uso di sistemi di sorveglianza biometrica nei luoghi pubblici, ii) l'utilizzo di sistemi di IA per la polizia predittiva e per il riconoscimento delle emozioni (c.d. *emotional based*). Il Parlamento UE ha posto l'attenzione sui diritti fondamentali dell'individuo, in particolare la *privacy* e riservatezza, al punto che sembra vietare il *predictive policing*; inoltre, ha posto le fondamenta per una normativa futura che eviti abusi di trattamento dei dati.

6.1 Affidabilità delle indagini mediante l'uso di algoritmi

La polizia predittiva basata sul luogo – intesa come innovazione della strategia investiva basata sui *big data*– dovrebbe essere il futuro del sistema investigativo. Ma almeno come attualmente inteso, l'analisi dei dati non mostra essere una certezza assoluta a livello di efficacia. I dati restano oscuri, per cui le questioni relative alla trasparenza dei processi conoscitivi delle macchine creano incertezza circa la completa affidabilità di questi nuovi sistemi predittivi. I tassi di criminalità, infatti sono talvolta aumentati e altre volte diminuiti nelle città che utilizzano sistemi come *PredPol*, *HunchLab*, *RTM* ecc. Ad esempio, utilizzando *PredPol*, durante un periodo di anno, da gennaio 2013 a gennaio 2014, la *Foothill Division* della polizia di Los Angeles (*LAPD*) ha assistito ad un calo del 20% del crimine previsto[214],ma, successivamente, nel 2015 e nel 2016, la criminalità è aumentata in tutta la città[215]. Per non parlare del fatto che mentre molte giurisdizioni hanno adottato la nuova tecnologia, alcune hanno interrotto l'uso di *PredPol* o altre ancora si sono completamente rifiutate di usufruire degli algoritmi predittivi, reputandoli pericolosi, in quanto il loro processo conoscitivo sfugge completamente al controllo umano, e inaffidabili[216].

Per testare l'efficacia della teoria predittiva, il *National Institute of Justice* ha finanziato il progetto pilota c.d. RAND a Shreveport, in Louisiana[217].L'obiettivo era quello di compiere una valutazione oggettiva circa l'efficacia della polizia predittiva basata sul luogo. In collaborazione con il dipartimento di polizia di Shreveport, i ricercatori hanno condotto uno studio di ventinove settimane utilizzando un algoritmo *ad hoc* progettato dagli analisti del crimine di Shreveport e dagli analisti del progetto RAND[218].

Simile ai sistemi *PredPol* ed RTM, il modello si è concentrato sui crimini contro la proprietà in aree segnalate come *hot-spot*, gli analisti hanno, altresì,

---

[214]Cfr., *A Los Angeles Police Department media report*, PredPol (a cura di), sul proprio sito web, PredPol, Management Team, *www.predpol.com*, 2017.
[215]Cfr., POSTON Ben, *Crime in Los Angeles Rose in All Categories in 2015, LAPD Says*, in *L.A. times* , 2015.
[216]Cfr., VUONG Zen, *Alhambra Police Chief Says Predictive Policing Has Been Successful*, in *Pasadena star-news*, 2014; AHUMADA Rosalio, *Modesto Sees Double-Digit Drop in Property Crimes-Lowest in Three Years*, in *Modesto Bee*, 2014.
[217]Cfr., HUNT Priscilla, SAUNDERS Jessica, & HOLLYWOOD John S., , *Evaluation of the shreveport predictive policing experiment* , in *RandCorp*, 2014, available at *www.rand.org*.
[218] *Ivi*, 4.

isolato particolari fattori geografici da inserire nel loro modello di rischio. I fattori di Shreveport includono:(i) la presenza di libertà vigilata o condizionale, (ii) *reports* circa tattiche di criminalità nei sei mesi precedenti, (iii)*reports* di previsioni criminali, (iv) chiamate al 911 per condotta disordinata, (v) vandalismo, (vi) arresti giovanili (vii) analisi durate 14 giorni sui risultati delle tattiche di prevenzione e dei maggiori fattori di rischio[219].

Dopo aver esaminato le informazioni e confrontato la previsione con il controllo, *RAND* ha concluso che "non c'era stato nessun impatto statisticamente significativo del programma sulla criminalità in generale, ma non è chiaro se ciò sia dovuto a un fallimento nel modello del programma o a un fallimento nell'attuazione del programma''[220]. In sostanza, lo studio effettuato da *RAND* non è riuscito a confermare o smentire l'efficacia o l'accuratezza della polizia predittiva, ma gli analisti restarono incerti sui motivi del fallimento della ricerca. Nonostante le perplessità, il controllo di determinati luoghi ''rischiosi'', alla base della teoria predittiva, dovrebbe funzionare, in vista della tendenza dei criminali ad essere individui abitudinari, che quindi tendono, come per ''l'effetto scossa''[221] a reiterare condotte già commesse e negli stessi luoghi. Ad esempio, a Boston, Massachusetts, per un periodo di sei anni, i ricercatori hanno scoperto che le sparatorie si sono verificate in una medesima area circoscritta[222]. Purtroppo, però, in questo caso la strategia predittiva si rivelò deludente. La polizia, infatti, aveva provveduto ad isolare le 13 aree bersaglio e a schierarvi unità di polizia speciali per pattugliare quei punti caldi (*hot-spots*), ma risultato fu che i crimini violenti accaddero ugualmente sia in quelle zone che in altri punti della città, trascurati dall'analisi algoritmica[223].

La teoria preventiva basata sul luogo viene spesso utilizzata anche per tracciare l'attività delle bande criminali. Si è evinto, negli Stati uniti, che le

[219]Cfr., FERGUSON, A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement,* in *NYU Press*, 2017, 71, *https://doi.org/10.2307/j.ctt1pwtb27.4*.
[220]*Ivi*, 33.
[221] V. paragrafo 4.4.1, Capitolo II.
[222]Cfr., PAPACHRISTOS Andrew, BRAGA Anthony A., & HUREAU David M., *Social Networks and the Risk of Gunshot Injury*, in *J. Urb. Health,* 2012, 89 , 992.
[223]*Ibidem.*

bande coinvolte in reati contro il patrimonio o legate allo spaccio di droga tendono a proteggere il territorio dagli altri gruppi criminali con violenza. Le bande ‘’attaccate ‘’ rispondono con altra violenza, portando a cicli di ritorsione di sparatorie potenzialmente senza fine[224]. Ma, sebbene questo meccanismo mostri un quadro sociale potenzialmente auto-distruttivo, la combinazione di territorialità e prevedibilità si traduce nella possibilità per la polizia per intervenire prima che la futura violenza si verifichi. Si può prevedere, quindi, che sparatoria avverrà in risposta a un'altra e lungo i confini territoriali. Uno studio sulle bande di Los Angeles ha rilevato che l'83% dei crimini di banda si è verificato all'interno di tre isolati da un noto confine di banda[225]. Sono state fatte, quindi, analisi simili su particolari club, bar e altri luoghi di ritrovo potenzialmente ‘’rischiosi’’, aiutando così la polizia ad un’azione preventiva più efficace.

Questi esempi mostrano la possibilità di illuminare l'oscurità che si cela dietro le attività criminali grazie al *data-driven policing*. Ma applicare quotidianamente questi sistemi, nel mondo reale resta assai difficoltoso sia per il continuo cambiamento dei meccanismi conoscitivi degli algoritmi che, grazie all’apprendimento automatico, mutano ogni giorno, sia perché resta incerta la concreta affidabilità delle macchine.

7. La predittività ad ausilio del sistema penale italiano

In una politica che tende a ridurre i costi della giustizia e a evitare il sovraccarico delle aule dei Tribunali, la giustizia predittiva[226] offre un’utile scorciatoia e trova applicazione efficientissima, nelle richieste di archiviazione. Il procedimento di archiviazione svolge un ruolo preminente nel processo

[224]Cfr., BROKAW Leslie, *Predictive Policing: Working the Odds to Prevent Future Crimes, Mitsloan Management Rev.*, 2011, available at *http://sloanre-view.mit.edu*.
[225]Cfr., SMITH Laura M. et al, *Adaption of an Ecological Territorial Model to Street Gang Spatial Patterns in Los Angeles*, in *Discrete & continuous dynamical sys*., 2012, 32, 3223; v. anche intervista con MOHLER George, in *Data sci. wkiy.* (*undated*), *www.datascienceweekly.org*.
[226]Cfr., Sul tema, in generale VIOLA L., voce *Giustizia predittiva*, in *“Diritto Online” Treccani*, 2018, CASTELLI C.– PIANA C., *Giustizia predittiva. La qualità della giustizia in due tempi*, in *questionegiustizia.it*; per un’analisi dell’esperienza francese GARAPON A., LASSÈGUE J., *Justice Digitale. Révolution graphique et rupture anthropologique*, Paris, 2018.

penale in quanto, scaturisce in seguito ad una notizia di reato infondata a seguito della quale appare chiaro al Giudicante che un rinvio a giudizio comporterebbe una inutile protrazione procedimentale, incoerente con il principio di economia processuale. L'art. 125 disp. Att. c.p.p.[227], in materia di archiviazione, stabiliva che: "vi è infondatezza della notizia di reato quando gli elementi acquisiti nelle indagini preliminari non sono idonei a sostenere l'accusa in giudizio"[228], oggi, a seguito della Riforma Cartabia, tale articolo è stato abrogato, e il criterio per l'archiviazione è sancito ai sensi dell'art. 408 comma 1 c.p.p. chiarendo che: ''il pubblico ministero chieda l'archiviazione, quando gli elementi acquisiti nelle indagini preliminari non consentono una ragionevole previsione di condanna o di applicazione di una misura di sicurezza diversa dalla confisca''. Questa circostanza impone l'emissione del provvedimento di archiviazione - provvedimento dovuto - perché espressione di un preciso dovere del p.m. indicato dall'art. 358 c.p. D'altro canto è semplicistico se non distorto, pensare che il pubblico ministero abbia come compito preminente solo quello di esercitare l'azione penale dal momento che, primaria è anche la sua funzione legata alla necessità di evitare di protrarre l'azione fino al dibattimento, ove, nel mentre del processo investigativo-accusatorio, fossero emersi degli elementi tali da far crollare i sospetti criminosi in capo ad un determinato soggetto indagato o imputato.

Tuttavia, molteplici sono i dubbi relativi all'applicazione del combinato disposto dell'art. 408 comma 1 c.p.p. e dell'art. 425 c.p.p. nel caso in cui vi sia una situazione di incertezza probatoria, relativamente all'esito della fase dibattimentale. Sul punto la Suprema Corte di Cassazione non ha fornito un orientamento univoco dal momento che se da un lato si è espressa nel senso che il rinvio a giudizio può essere disposto anche nel caso in cui vi sia una previsione, "astrattamente possibile" che si arrivi ad una sentenza di condanna, dall'altro ha ritenuto indispensabile per il rinvio a giudizio, l'aver acquisito un

[227]Cfr., VIOLA L., voce *Giustizia predittiva,* in *"Diritto Online" Treccani,* 2018, CASTELLI C. – PIANA C., *Giustizia predittiva. La qualità della giustizia in due tempi,* in *questionegiustizia.it*; per un'analisi dell'esperienza francese GARAPON A., LASSÈGUE J., *Justice Digitale.Révolution graphique et rupture anthropologique*, Paris, 2018.
[228]Cfr., PARODI Cesare e SELLAROLI Valentina, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo (DPC)*, 2019, VI, 63.

quadro probatorio che consenta di prevedere tale esito, non potendo il Giudice disporre il proscioglimento in tutti quei casi in cui le prove acquisite, a carico dell'imputato si prestino a soluzioni alternative o potrebbero essere valutate in maniera diversa nella fase dibattimentale [229].In questo contesto, l'esame dei dati raccolti, quindi anche mediante analisi predittiva, costituisce per le Procure un grosso supporto relativamente alla previsione dell'esito processuale. Tuttavia, l'affidarsi a dati elaborati da un software, se da un lato ottimizza le risorse degli uffici giudiziari, dall'altro potrebbe condurre ad una "spersonalizzazione"[230] degli stessi, con conseguente scarso controllo sui dati e quindi rischi di incorrere in errori, soprattutto legati al fatto che spesso questi sistemi predittivi creano problemi di trasparenza legati all'oscurità del loro funzionamento e del loro meccanismo conoscitivo.

Per evitare ciò, sono stati adottati dei correttivi al sistema giudiziario che consistono: (i) nella facoltà del Pm o del GIP di non rendere noto il giudizio predittivo di colpevolezza o di condividerlo con delle integrazioni e/o modifiche; (ii) di accettare un minimo grado di spersonalizzazione al fine di ridurre il carico dei processi, e al fine di concentrare le risorse del sistema giudiziario sui processi, senza mai trascurare l'obbligatorietà dell'azione penale; (iii) nel risolvere le questioni di trasparenza relativamente al funzionamento degli algoritmi predittivi; (iv) infine, nel mettere anche a disposizione dei difensori, gli strumenti di predizione, al fine di consentire loro di fare previsioni circa l'esito del dibattimento, e ciò per far anticipare, ai propri assistiti, le possibilità di subire una condanna e/o per consigliare loro riti alternativi, con la conseguenza di rendere più trasparente il rapporto imputato-difensore. Questo meccanismo predittivo-preventivo potrebbe giovare al sistema giudiziario in generale, mediante una complessiva riduzione dei processi.

---

[229]Cfr., Cass., Sez. II, n. 46145, 5 novembre 2015, CED 265246; conf. Cass., sez. II, n. 15942, 7 aprile 2016, n. 15942, CED 266443; Cass., sez. II, n. 48831, 14 novembre 2013, n. 4883, CED257645Cass, Sez. VI, n. 33763, 30 aprile 2015, CED 264427; Cass., Sez I, n. 7748, 11 novembre 2015, CED266157.

[230]Cfr., PARODI Cesare e SELLAROLI Valentina, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo (DPC*), fascicolo n. VI, 2019, 63 ss.

Resta ora da esaminare un altro aspetto: l'applicabilità delle elaborazioni statistiche dell'intelligenza artificiale, ai processi, relativamente alla valutazione predittiva della pericolosità e le successive conseguenze impattanti sul singolo individuo.

In buona sostanza, si tratta di capire se gli algoritmi predittivi basati sul rischio possano stimare se un individuo commetterà un nuovo reato, o possano essere d'ausilio per la valutazione dell'applicabilità di una misura cautelare (art. 274 lett. c, c.p.p.), una misura di sicurezza (art. 202 c.p.) o una misura di prevenzione (art. 6 d. lgs.159/2011), tramite una analisi di pericolosità caso per caso.

Per essere utilizzati e costituire un valido supporto al giudice, la decisione sulla pericolosità non deve essere rimessa totalmente alle elaborazioni del programma; le elaborazioni debbono essere poste a disposizione del Giudice e devono essere da lui verificate. I dati inseriti, nell'analisi, non devono essere estranei alla personalità del soggetto e il valore predittivo, non potrà essere condizionato da fattori di genere, sociali, etnici o economici, altrimenti si incorrerebbe in valutazioni pregiudizievoli. Qualora queste regole non vengano rispettate, i dati non potranno essere utilizzati, così come le analisi algoritmiche perché contrari ai principi costituzionali oltre che non conformi alle indicazioni della CEDU.

Ma quali dati sono utilizzabili? Una decisione non può assolutamente dipendere o derivare dall'indagine della sola macchina, senza il controllo umano che confermi affidabilità dei dati. Bisogna precisare che i dati, per essere credibili, devono essere aderenti alla realtà da interpretare ed inerenti allo scopo da ottenere. Purtroppo, i dati non sempre sono di qualità, soprattutto nel caso in cui gli sviluppatori e utilizzatori di questi algoritmi non dispongono di dati diretti, o perché non ne esistono ancora o, perché non ne hanno accesso, o perché spesso usufruiscono di dati *online* spesso erronei. Questi dai sono i c.d. *proxi data o dati indiretti o vicarianti*[231]che, rendono la qualità delle notizie raccolte, non del tutto accurata. Si pensi, ad esempio, al modello matematico

[231]Cfr., Su tutto il tema dei dati vicarianti e del problema posto dai *proxy data* nell'uso dei modelli matematici si veda il volume di O'NEIL Cathy *Weapons of Math Destruction*.

sviluppato dalle Banche per prevedere se un soggetto sarà in condizione di restituire un prestito. Se all'interno del programma vengono inseriti dati connessi a tale previsione, quali la mancanza di versamento di rate di mutuo, o una complessiva inadempienza contrattuale, ma vengono aggiunte anche informazioni non pertinenti al caso(i c.d. dati vicarianti) come dati relativi all'età, al codice postale, alla residenza, al grado di scolarità ecc., si incorre necessariamente in confusione a causa del fatto che non tutti i dati sono accurati ed efficaci per l'analisi del caso specifico, e conducono, così, a valutazioni fuorvianti e/o discriminatorie (ad esempio associando la residenza ad un quartiere tendenzialmente povero).

Vi sono poi, situazioni in cui non si dispone neppure dei c.d. dati ''indiretti'' e allora si fanno le c.d. valutazioni *bucket* (secchio), in cui non vengono esaminati dati relativi alla singola persona, ma alle categorie cui appartengono, quindi il lavoro, le relazioni con i colleghi ecc, è chiaro che queste analisi rischiano ancor di più di risultare erronee.

In virtù di quando espresso, la considerazione finale che ne deriva è che i dati, per essere utili in qualsiasi indagine conoscitiva, devono essere pertinenti, di qualità, cioè derivanti da fonti certe ed affidabili, deve conoscersi la loro provenienza e non devono essere manipolabili. In aggiunta si deve mirare ad una programmazione algoritmica in un'ottica di trasparenza circa il funzionamento del *software*, per evitare oscurità sul procedimento di apprendimento automatico delle macchine e quindi una mancanza di controllo dell'essere umano.

CAPITOLO III

LA TECNOLOGIA DEL RICONOSCIMENTO FACCIALE

Negli anni recenti, nell'esperienza americana e non solo, si è assistito al sempre più frequente utilizzo delle tecniche di riconoscimento facciale o biometrico da parte delle forze dell'ordine.

Prima di esaminare l'evoluzione di questi algoritmi, bisogna chiarire il concetto di biometria[1] che viene definita come la ''disciplina che studia le grandezze biofisiche, allo scopo di identificarne i meccanismi di funzionamento, di misurarne il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici"[2]. In buona sostanza, la biometria, è una scienza che viene utilizzata per identificare o riconoscere le persone e, ad oggi, è utilizzata per le attività di c.d. autenticazione biometrica, sulla base di osservazioni anatomiche, fisiologiche, comportamentali o altre caratteristiche, come ad es. la voce mediante il ''riconoscimento vocale''[3]. La scienza biometrica è stata usata inizialmente per le impronte digitali, poi è stata applicata alla geometria della mano che ne rileva la forma, la lunghezza e la larghezza. Di recente si stanno sviluppando anche tecniche biometriche che esaminano l'iride e la retina.

---

[1] Voce "Biometria", in *Enciclopedia Treccani online*.

[2] Cfr., CURRAO Elettra, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *DPU—Diritto Penale Uomo,*2021, 5, 2 ss.

[3] Il funzionamento del sistema si snoda in due passaggi essenziali: A) Fase di registrazione del dato biometrico (c.d.*enrollment*):si procede alla rilevazione e all'acquisizione dell'informazione biometrica sotto forma di dato biometrico grezzo. Quest'ultimo viene poi rappresentato come modello (c.d. *template*), così da potere essere archiviato e confrontato con i dati già acquisiti. B) Fase di verificazione del *template*: questo passaggio si basa sulla comparazione tra i *templates* già presenti nel sistema e quelli acquisiti istantaneamente a seguito dell'interazione con l'utente. Tale fase è, dunque, finalizzata a verificare la coincidenza o meno tra i dati e, nel caso di esito positivo, il sistema ne decreterà il *matching*. Occorre precisare che non vi potrà mai esservi piena coincidenza tra i dati, in quanto l'uno e l'altro saranno rappresentati secondo formule matematiche diverse (considerato il differente momento della rilevazione). Per tale ragione, il sistema si basa su risultati di coincidenza approssimativi e fornisce un determinato punteggio, che, a seconda del superamento o meno di una soglia predeterminata di somiglianza, viene registrato come risultato di "match" o di *"not match";* SACCHETTO E., *Nuove Tecnologie e processo penale,* in *DPC—*

Diritto penale contemporaneo, 2019, 2, 468 ss.

Ciò chiarito, è ora possibile esaminare, più nel dettaglio, come funzionano nella prassi le tecniche di riconoscimento facciale.

Il riconoscimento facciale è una tecnica algoritmica grazie alla quale le macchine rilevano ed interpretano immagini. Come vedremo, sebbene si tratti di una tecnica straordinaria, derivano ingenti dubbi interpretativi[4].

Le modalità con cui le TRF agiscono consistono nell'analisi automatizzata di immagini digitali che illustrano il volto di una persona. Mediante i dati raccolti (*big data tecnology*), grazie alle tecniche biometriche, si ricavano caratteristiche sui tratti distintivi del volto che, poi, sono tradotti in forma di codici alfanumerici ed eventualmente arricchiti da indici ulteriori (*hashing*)[5].

L'autenticazione/verifica può avvenire in varie modalità: il volto può essere abbinato alla foto o dal vivo, ad esempio con un documento di identità; può essere abbinatoalle foto raccolte in un *database* per individuarne la corrispondenza (*match*); i volti possono essere, infine, individuati utilizzando i filmati (*frame*) estrapolati da telecamere a circuito chiuso, per poi confrontarli con le immagini presenti negli appositi *database* di ricerca, con lo scopo di trovare un *match*[6].

In tutti i casi sopra descritti, viene utilizzato un *software* con il quale si identifica una persona ''segnalata'' isolando le caratteristiche tipiche del volto[7].

Queste rilevazioni possono essere effettuate sia in modalità ''da remoto'', sia in tempo reale, anche se viene privilegiata la modalità *ex post*, ossia mediante l'analisi di file video/immagine archiviati.

Ma come si istruiscono le macchine alla comprensione e alla raccolta di dati?

---

[4]Cfr., CRAWFORD K., *Né intelligente né artificiale. Il lato oscuro dell'IA*, Il Mulino, Bologna, 2021, p. 119 ss.

[5]Sul funzionamento delle TFR, *cfr.,* MOBILIO G., *Tecnologie di riconoscimento facciale,* cit., p. 32ss.; v. anche BUOLAMWINI J. – ORDONEZ V. – MORGENSTERN J.– LEARNED-MILLER E., *Facialrecognitiontechnologies: a primer, Algorithmic Justice League,* 2020, (a cura di), in *https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf.*

[6]Cfr., CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *Diritto Penale Uomo—DPU*, fascicolo n. 2021, 5, 2 e 5.

[7]Cfr., ZUBOFF S., *The age of surveillance capitalism,* 2019 cit., 353 ss.

L'analisi inizia dalla raccolta di molteplici campioni di immagini che, dopo essere state opportunamente catalogate, vengono etichettate e correlate in maniera induttiva o su base statistica; ciò al fine di ottenere un progressivo affinamento del processo conoscitivo autonomo della macchina volto ad individuare le similitudini tra i dati raccolti, in relazione allo scopo da raggiungere[8]. Più nel dettaglio, una volta inserite nel sistema le immagini, grazie ad un algoritmo (*learner*), lo stesso viene programmato per apprendere e trasmettere i dati ad un secondo algoritmo (*classifier*) che individua le relazioni tra i nuovi *input* immessi e gli *output* autonomi attesi.

Quanti più dati si ottengono, tanto più il risultato elaborato dalla macchina sarà preciso. Da ciò deriva la raccolta ''selvaggia'' dei dati in rete, spesso effettuata senza alcun consenso, o l'utilizzo per scopi identificativi di *database* già esistenti e concepiti per altri utilizzi; il tutto finalizzato ad "alimentare" di immagini, le c.d. macchine "ingorde[9]" che sono programmate per il riconoscimento facciale.

Da tale meccanismo, alquanto distorto, sono derivate innumerevoli problematiche connesse alla violazione della *privacy* delle persone le cui foto sono state utilizzate per allenare i sistemi di riconoscimento facciale[10] nonché alla scarsa affidabilità dei sistemi, derivante dalla varietà dei dati e dalla scarsa correttezza delle classificazioni.[11]In particolare, sono stati evidenziati i frequenti *racial bias,* legati al fatto che questi *software* sono meno allenati a riconoscere persone di determinati genere o colore della pelle[12]. Su questo

[8]V., QUINTARELLI S., *Intelligenza artificiale. Cos'è davvero, come funziona, che effetti avrà, Bollati Boringhieri,* (a cura di), *Milano, 2020;* CHIRIATTI M., *Incoscienza artificiale. Come fanno le macchine a prevedere per noi,* in *Luiss University Press, Roma,* 2021.

[9]Cfr., CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *Diritto Penale Uomo—DPU,* 2021, 5, 2 e 5.

[10]Cfr., CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *Diritto Penale Uomo—DPU,* 2021, 5, 2 e 5.

[11]Cfr., COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini,* in *Sistema Penale —SP,* 2022, 9, 30 ss.

[12]Cfr., IVANOVA I., *Why face-recognition technology has a bias problem,* in *www.cbsnews.com,* 2020.

punto le aziende hanno cercato di migliorare l'efficacia degli algoritmi facciali ampliando la tipologia di dati a cui fanno ricorso[13].

Naturalmente, questo *modus operandi*, diretto a correggere problematiche connesse ai sistemi di intelligenza artificiale, è stato spesso contrastato, in quanto si è ritenuto che «Le pratiche di classificazione danno forma al modo in cui l'intelligenza artificiale viene classificata e prodotta (…) tutto ciò che esiste al mondo viene convertito in dati attraverso l'estrazione, la misurazione, l'etichettatura e l'ordinamento, e questo diventa, intenzionalmente o meno, una scivolosa evidenza empirica per i sistemi tecnologici addestrati su questi dati»[14].

Infatti, si è evidenziato che le TFR riducono l'individuo a un mero dato numerico, tramite il processo di "datificazione", e sono programmate classificare il genere umano in modo artificiale. Tali modalità sviliscono l'individuo ed i suoi diritti fondamentali.

Tuttavia, gli avanzamenti scientifici e i percorsi evolutivi in ambito di *facial recognition* aumentano di giorno in giorno; la scienza biometrica è, per questo, seppur con discrete criticità, utilizzata di frequente (in particolare in stati come Gli Stati Uniti, la Cina, e anche in Europa seppur con svariate limitazioni) nell'ambito della sicurezza pubblica, della prevenzione al crimine e dei procedimenti investigativi e, in generale, della repressione della delinquenza mediante appositi software di *face-matching*. Questi sistemi sono programmati con lo scopo specifico di associare le immagini del volto degli individui che transitano per le strade cittadine, con quelle presenti nei *database* di polizia contenenti foto di soggetti ''segnalati''. L'obiettivo, quindi, come nei meccanismi applicativi dei *software* di identificazione e autenticazione[15] basati

[13]V. ROACH J., *Microsoft improves facial recognition technology to perform well across all skin tones, genders,* 2018, sito della *Società Microsoft*, nonché R. PURI, *Mitigating Bias* in *AI Models,* in *IBM*, 2018

[14]CRAWFORD K., *Né intelligente né artificiale, Bologna,* 2021 cit., 144.

[15]Cfr., COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema Penale —SP*, 2022, 9, 30 ss.

sui dati biometrici, è ottenere una corrispondenza (*matching*) tra i dati c.d. ''sconosciuti'', e i dati ''noti'' alle forze dell'ordine[16].

La tecnologia del riconoscimento facciale, attualmente, viene spesso utilizzata dai privati, per attività proprie, come ad esempio per la videosorveglianza all'interno degli esercizi commerciali[17], o per azioni collaborative con la polizia. L'uso di vere e proprie telecamere intelligenti, capaci di effettuare operazioni di riconoscimento e autenticazione[18], si traduce nella creazione di veri e propri sistemi di controlli, capaci potenzialmente di identificare tutti gli esseri umani tracciati ''dall'occhio digitale''.

[16]Cfr. *European Union Agency for fundamental rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, Fra Focus,* 2019, 2.

[17] Cfr., CURRAO Elettra, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *Diritto Penale Uomo—DPU,* 2021, 5, 4 e 5.

[18]È il caso del supermercato intelligente *Amazon Go inaugurato a Seattle* nei primi mesi del 2018, in fase di sperimentazione dal 2017. V., MANTOVANI R., *Digital Life, Il supermercato ti riconosce dalla faccia,* in *Focus,* 2017.

Estremamente innovativo è l'utilizzo delle tecnologie di riconoscimento facciale per finalità di c.d. *neuromarketing*[19]o per controllo dei luoghi di lavoro, come strumenti di riconoscimento dei lavoratori e i c.d. *badge*, o degli aeroporti, il c.d. *face boarding*[20]. Uno dei primi esperimenti effettuati da privati, è stato quello della Disney che ha utilizzato sistemi di riconoscimento facciale per "leggere" i volti degli spettatori durante la proiezione dei film (i c.d. *emotion recognition system*[21]) e cogliendo le diverse espressioni facciali, questi sistemi sono in grado di tradurre il tratto facciale in stato emotivo. In questo modo la Disney riesce, tutt'ora a comprendere il grado di apprezzamento dei nuovi film e tracciare gli aspetti che sono di maggior gradimento per riproporli e quelli di minore impatto, migliorandoli[22].

2. Sistemi di *face surveillance*

Un'innovazione tecnologica che ha attirato molta attenzione negli ultimi anni è proprio la tecnologia del riconoscimento facciale[23].

L'idea alla base dei sistemi di riconoscimento facciale è quella di associare un'immagine digitale, memorizzata in appositi database, ad un volto di un individuo sospettato o potenzialmente criminale o, in generale, di monitorare

---

[19] L'utilizzo di sistemi di riconoscimento facciale è frequente nell'ambito del c.d. *marketing* comportamentale.

[20] L'aeroporto di Linate col progetto *"Face Boarding"* si appresta a sperimentare sistemi di *face boarding,* basati su uno *screening* facciale del passeggero, con significativa riduzione dei tempi di imbarco e semplificazione delle procedure.

[21]Cfr., CURRAO Elettra, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *Diritto Penale Uomo—DPU*, 2021, 5, 5.

[22] Si tratta dei c.d. *«emotion recognition system»* a cui fa riferimento la recentissima proposta di Regolamento presentata dalla Commissione Europea in data 21 aprile 2021. V., *amplius* COLDEWEY D., *This facial recognition system tracks how you're enjoying a movie*, in *TechCrunch*, 2017.

[23]Cfr., GARVIE CLARE, BEDOYA ALVARO M. & FRANKLE JONATHAN, GEORGETOWN L. in *Priv. & Tech., the perpetual line-up: unregulated police face recognition in America*, 2016, 1, *https://www.perpetuallineup.org/sites/default/files/2016-12/The% 20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf, [https://perma.cc/S48P -PL53;* .CAGLE Matt & OZER Nicole A., *Amazon Teams Up with Law Enforcement To Deploy Dangerous New Face Recognition Technology*, in *ACLU N. CAL.*, 2018, *https://www.aclunc.org/blog/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology [https://perma.cc/WYF4-7XDT*]; v. anche SPIELMAN Fran, *ACLU Sounds the Alarm About Bill Allowing Use of Drones To Monitor Protesters*, in *Chi.sun-times*, 2018, 5:17 PM, *https://chicago.suntimes.com/politics/aclu-sounds-the-alarm-about-bill-allowing-use-of-drones-to-monitor-protesters [https:// perma.cc/T64R-SS94*].

le città e le persone a livello generalizzato[24]. Per il c.d. ''*matching'',* il programma, installato su computer avanzati, opera analizzando le fotografie digitali registrate dalle telecamere di videosorveglianza creando una rete digitale di tracciabilità e identificazione mirata[25]. Il riconoscimento facciale è, quindi, definibile come ''tecnologia di corrispondenza digitale''[26].In pratica, le immagini digitali dei volti vengono suddivise in piccoli ''frame'', con l'intento di studiare, in modo specifico, i dettagli dei tratti facciali[27].

Tradizionalmente, infatti, la tecnologia di riconoscimento facciale nasce come una scienza basata sia sulle ''caratteristiche'' (''*feature-based*''), intese come gli occhi, il naso e la bocca e le distanze tra queste caratteristiche del volto[28], che "sull'aspetto'' (c.d.*''appearance-based"*), inteso come la complessiva corrispondenza dell'immagine all'intero volto. Negli ultimi anni sono emerse altre forme di identificazione che analizzano le caratteristiche della pelle[29], le ombre[30], i modelli tridimensionali[31], o una combinazione di tutti questi elementi[32].

---

[24]Cfr., LEVASHOV Kirill, *The Rise of a New Type of Surveillance for Which the Law Wasn't Ready*, in *Colum. sci. & tech. l. rev.*, 2013, 164, 167–168, 15; GARVIE Clare & FRANKLE Jonathan, *Facial-Recognition Software Might Have a Racial Bias Problem*, in *Atlantic* 2016, *https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991, [https://perma.cc/4L5J -AXR4]*.

[25]Cfr., BUOLAMWINI JOY, ORDÓÑEZ VICENTE, MORGENSTERN JAMIE & LEARNED MILLER ERIK, *Facial Recognition Technologies: a primer,* 2020, 8 e 13, *https://global-uploads.webflow.com/5e027cal88c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf, [https://perma.cc/X8CH-JAV3]*.

[26]Cfr., FERGUSON, Andrew Guthrie, *Facial Recognition and the Fourth Amendment*, 2019. in *Minnesota Law Review*, 2021, 1105, 106, *https://ssrn.com/abstract=3473423* or *http://dx.doi.org/10.2139/ssrn.3473423*.

[27]Cfr., "*In the Face of Danger: Facial Recognition and the Limits of Privacy Law*.",in *Harvard Law Review,* 2007, vol. 120, 7, 1870 e 1891, *http://www.jstor.org/stable/40042639.*

[28]Cfr., JOSHI Jagdish Chandra & GUPTA K.K., *Face Recognition Technology*: A Review, in *Jup j. Telecomms* 2016, 53, 54, 8 ; GALTERIO Mary Grace, SHAVIT Simi Angelic & HAYAJNEHT haier, *A Review of Facial Biometrics Security for Smart Devices,* in *MDPI Computers* 2018, 37, 3, 7; RELLY Victoria, PETRESCU Virgil, *Face Recognition as a Biometric Application,* in *J. Mechatronics &Rrobotics* 2019, 237-240, 3 .

[29]V. RELLY Victoria, PETRESCU Virgil, *Face Recognition as a Biometric Application,* in *J. Mechatronics & Robotics,* 2019, 237-241, 3.

[30]V. GALTERIO Mary Grace, SHAVIT Simi Angelic & HAYAJNEH Thaier, *A Review of Facial Biometrics Security for Smart Devices, MDPI Computers* 2018, 7, 37,3 .

[31]V. RELLY Victoria, PETRESCU Virgil, *Face Recognition as a Biometric Application,* 3 *J. Mechatronics & Robotics* , 2019, 3, 240 ss.

[32]*Ivi*, 241.

In sostanza, l'impronta ‘’facciale’’ (*faceprint*) è comparata, per la rilevazione dell’identità, ad un'impronta digitale (*fingerprint*); in altre parole, il sistema di individuazione è codificato in modo da misurare la distanza tra lineamenti, linee ed altri elementi facciali, così come accade con il confronto delle impronte delle dita[33]. Per verificare che la ‘’corrispondenza’’ tra un volto tracciato in *real-time* e l’immagine digitale sia corretta, questi programmi sovrappongono i due *frame* fotografici e, se i modelli si allineano perfettamente, vuol dire che costituiscono un *match*, quindi una conferma che si tratta del medesimo soggetto[34].

Queste immagini digitalizzate sono memorizzate in grandi *datasets* in modo che il modello computerizzato di riconoscimento possa addestrarsi, tramite la tecnologia di *machine-learning*, ad imparare gli elementi che costituiscono una corrispondenza[35].

Tuttavia, questi sistemi, spesso, confrontando le caratteristiche facciali, associano molti *matches* di volti ad una sola immagine digitale, a causa di somiglianze tra loro[36]. Quindi, per esempio, un agente di polizia che cerca un riscontro con una fotografia di un sospettato può ricevere da venti a cinquanta impronte facciali come possibili riscontri, rendendo difficile individuare quella utile alle indagini[37].

---

[33]Cfr., LEVASHOV Kirill, *The Rise of a New Type of Surveillance for Which the Law Wasn’t Ready*, in *Colum. Sci. & Tech*. 2013, 15, 164, e 167 ss.

[34]Cfr., BUOLAMWINI JOY, ORDÓÑEZ VICENTE, MORGENSTERN JAMIE & LEARNED ERIK MILLER, *Facial recognition technologies: a primer*, 2020, 10 e 14, *https://global-uploads.webflow.com/5e027cal88c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf [https://perma.cc/X8CH-JAV3]*.

[35]Cfr., GARVIE CLARE, BEDOYA ALVARO M. & FRANKLE JONATHAN, *GEORGETOWN* in *Priv. & Tech.*, *The perpetual line-up: unregulated police face recognition in America*, 2016, 9, *https://www.perpetuallineup.org/sites/default/files/2016-12/The% 20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technol-ogy%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/S48P -PL53*].

[36]Cfr., BUOLAMWINI JOY, ORDÓÑEZ VICENTE, MORGENSTERN JAMIE & LEARNED ERIK MILLER, *Facial recognition technologies: a primer*, 2020, 12, *https://global-uploads.webflow.com/5e027cal88c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf [https://perma.cc/X8CH-JAV3]*.

[37]Cfr., GARVIE CLARE, BEDOYA ALVARO M. & FRANKLE JONATHAN, *GEORGETOWN* in *PRIV. & TECH.*, *The perpetual line-up: unregulated police face recognition in America*, 2016, 9, *https://www.perpetuallineup.org/sites/default/files/2016-12/The% 20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technol-ogy%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/S48P -PL53*].

Per questo motivo, per una efficace resa, i sistemi devono ''auto-addestrarsi'' ad esaminare i volti e a classificarli, in modo da identificare i punti focali di similitudine realmente incriminanti[38]. Per cui, dopo che il programma avrà creato un elenco di impronte facciali corrispondenti, un analista specializzato *ad hoc* esaminerà le immagini per selezionare il sospetto ''finale'' dell'indagine (se presente nell'elenco)[39].

La tecnologia di riconoscimento facciale è disponibile in forme diverse e può essere utilizzata per scopi diversi[40].

Esistono molti sistemi quali:

(i) la sorveglianza facciale che comporta l'identificazione di una massa generalizzata di individui utilizzando la tecnologia di riconoscimento facciale; spesso viene applicata in Cina[41];

(ii) l'identificazione del volto, che prevede l'abbinamento di un particolare volto (un sospetto) a un database di fotografie esistenti (un database di foto segnaletiche o registri della motorizzazione)[42]. L'identificazione facciale, in particolare, è stata sperimentata dalla polizia come uno strumento investigativo rivoluzionario simile alla corrispondenza del DNA[43] ed è anche sperimentata in alcuni luoghi commerciali per migliorare la sicurezza privata[44];

---

[38]Cfr., *U.S. GOV'T ACCOUNTABILITY OFF.*, GAO 15-621, *Facial recognition technology: commercial uses, privacy issues, and applicable federal Law,* 2015, 3 s.,*http:// www.gao.gov/assets/680/671764.pdf [https://perma.cc/U9GG-J7NS]*.

[39]Cfr., WILTZ Teresa, *Facial Recognition Software Prompts Privacy, Racism Concerns in Cities and States,* in *Pew Statelin*, 2019, *https://www.pewtrusts.org/en/ research-and-analysis/blogs/stateline/2019/08/09/facial-recognition-software-prompts-privacy-racism-concerns-in-cities-and-states [https://perma.cc/4RJU -CV88]*.

[40]V., GALTERIO et al., nota 5, 3 s.

[41]Cfr., FERGUSON, Andrew Guthrie, *Facial Recognition and the Fourth Amendment*, 2019. in *Minnesota Law Review,* 2021, 1105, 108, *https://ssrn.com/abstract=3473423* or *http://dx.doi.org/10.2139/ssrn.3473423*.

[42]Cfr., BUOLAMWINI Joy, *Response: Racial and Gender Bias in Amazon Rekognition— Commercial AI System for Analyzing Faces*, in *Medium,* 2019, *https://medium .com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced [https://perma.cc/U2F3 -LT4T]* ("Facial identification . . . involves trying to match a face to a person of interest in an existing database of faces.").

[43]Cfr., BARBASCHOW Asha, *How One Sheriff's Office Is Using Machine Learning to Uncover Persons of Interest,* in *ZDNET*, 2017, *https://www .zdnet.com/article/how-one-sheriffs-office-is-using-machine-learning-to-uncover -persons-of-interest [https://perma.cc/L9RY-NE3F]*.

[44]Cfr., FRANCE Lisa Respers, *Taylor Swift Reportedly Used Facial Recognition to Try to ID Stalkers*, in *CNN* , 2018, *https://www.cnn.com/2018/12/13/ entertainment/taylor-swift-facial-recognition/index.html [https://perma.cc/F9PW -NMQ3]*.

(iii) il tracciamento facciale (*''face tracking''*), poi, è un ibrido di sorveglianza facciale e identificazione facciale[45]. Il tracciamento dei volti implica l'uso da parte della polizia di video archiviati o registrazioni, in tempo reale, per rintracciare un sospetto preso di mira[46]. Ad esempio, dopo una rapina in banca, la polizia potrebbe cercare nei *feed* video della città per trovare riscontro circa il percorso utilizzato dal sospetto per la fuga[47].

C'è una importante differenza tra il rilevamento del volto e l'identificazione del volto che consiste nel fatto che il rilevamento del volto fornisce informazioni circa la posizione del sospetto, l'identificazione invece si limita al mero *matching* tra foto segnaletiche registrate nei *database* e video in tempo reale.

(iv) Infine, occorre citare brevemente anche un altro sistema: la ''verifica del volto'' che consiste nella successiva conferma che un particolare volto umano presente davanti alle telecamere corrisponda a un'immagine digitale preimpostata di quel volto[48].

È doveroso esaminare nel dettaglio le tecnologie di sorveglianza facciale, di identificazione facciale e di tracciamento facciale.

La sorveglianza facciale comporta il monitoraggio generalizzato di luoghi pubblici o di set di immagini, per poi confrontarli con un elenco precompilato dal governo degli Stati Uniti contenente le fotografie dei volti dei detenuti[49]. Le metodologie con le quali la polizia si avvale della sorveglianza facciale sono tre: (i) scansione delle riprese video memorizzate e successiva identificazione di tutti i volti registrati; (ii) scansione e identificazione del viso in tempo reale

---

[45]., FERGUSON, Andrew Guthrie, *Facial Recognition and the Fourth Amendment*, 2019. In *Minnesota Law Review*, 2021, 1105, 109, *https://ssrn.com/abstract=3473423* or *http://dx.doi.org/10.2139/ssrn.3473423*.

[46]Cfr., Cfr., GARVIE CLARE, BEDOYA ALVARO M. & FRANKLE JONATHAN, *GEORGETOWN* in *Priv. & Tech., The perpetual line-up: unregulated police face recognition in America*, 2016, 12, *https://www.perpetuallineup.org/sites/default/files/2016-12/The% 20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technol-ogy%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/S48P -PL53*].

[47]*Ibidem.*

[48]Cfr., LOCKLEAR Mallory, *DHS Will Use Facial Recognition To Scan Travelers at the Border*, in *Engadget* , 2018, *https://www.engadget.com/2018/06/05/dhs-facial -recognition-scan-travelers-at-border [https://perma.cc/V4E8-7N7M]*; PETRESCU Virgil, *Face Recognition as a Biometric Application,* in *J. Mechatronics &Robotics* 2019, 237-240, 3

[49]Cfr., NAKAR Sharon & GREENBAUM Dov, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, in *B.U.J. Sci. & Tech*, 2017, 88-94, 23

tramite la videosorveglianza; (iii) il *data mining* di immagini memorizzate da piattaforme di terze parti, per individuare determinate persone attraverso le loro fotografie.

È necessario analizzare questi metodi investigativi nel dettaglio.

La scansione delle riprese video memorizzate consiste nel ricercare e successivamente nell'esaminare i video, delle telecamere di sorveglianza in rete, archiviati[50]. In parole semplici, si tratta di identificare determinate persone segnalate mentre, ad esempio, camminano per strada, o viaggiano su mezzi pubblici o con la propria automobile[51].

Queste telecamere, che memorizzano dati, possono essere di proprietà del governo, di privati o provenire da dispositivi mobili come, ad esempio, le videocamere indossate dalla polizia (*police-worn body cameras*[52])[53]. Uno dei vantaggi, derivante dall'uso di questi sistemi, consiste nel fatto che l'archiviazione, essendo digitalizzata e quindi non più cartacea, diventa più economica ed accessibile con maggiore facilità e velocità. Questa tipologia di sorveglianza facciale è in grado, quindi, potenzialmente, di abbinare qualsiasi volto, avente le medesime caratteristiche di un altro inserito nel set di dati governativo preregistrato, creando, così, una corrispondenza e quindi una conferma circa la medesima identità. Tuttavia, per chiarezza, è necessario precisare che la ricerca dei riscontri nei filmati archiviati non si basa necessariamente su un sospetto individualizzato di un crimine o per supportare

---

[50]Cfr., GARVIE Clare & MOY Laura, *America Under Watch: Face Surveillance in the United States*, in *Geo. Ctr. on priv. & tech.: am. under watch*, 2019, *https:// www.americaunderwatch.com [https://perma.cc/P6RF-56EB*] (describing how various police departments use a network of surveillance cameras to conduct face surveillance).

[51]Cfr., GROSS Allie, *Experts: Duggan's Denial of Facial Recognition Software Hinges on 3 Words*, in *Det. Free press*, 2019, *https://www.freep.com/story/ news/local/michigan/detroit/2019/07/16/duggan-war-of-words-surveillance-tech/1701604001 [https://perma.cc/9N2H-U7HW*] (describing how the Detroit Police Department's facial recognition technology takes still images from videos to find a match).

[52]V. paragrafo 5, Capitolo II.

[53]Cfr., BURT Chris, *Motorola Could Offer Facial Recognition with Police Body Cam- eras with WatchGuard Acquisition*, in *Biometric Update*, 2019, *https://www.biometricupdate.com/201907/motorola-could-offer-facial-recognition-with-police -body-cameras-with-watchguard-acquisition [https://perma.cc/6RQG-EHGP]*. *But see* Madeline Purdue, *Axon Body-Camera Supplier Will Not Use Facial Recognition in Its Products – For Now*, in *USA today*, 2019, 2:17 PM, *https://www.usatoday.com/story/tech/2019/07/01/axon-rejects-facial-recognition-software-body-cameras -now/1601789001 [https://perma.cc/324C-AALN]*.

una particolare indagine penale, pur essendo utilizzabile anche per questi scopi, ma nasce semplicemente per creare un monitoraggio generalizzato degli individui a mezzo di videosorveglianza[54]. Le scansioni, registrate dalle telecamere, potrebbero, a lungo termine, localizzare i cittadini in qualsiasi punto in cui vengono identificati, creando una mappa retrospettiva virtuale di movimenti e attività nel tempo[55].

Un'altra forma di tecnologia di sorveglianza facciale è il monitoraggio pubblico in tempo reale. La tecnologia viene utilizzata, di frequente, in Paesi come la Cina, per osservare le strade e identificare le persone negli spazi pubblici utilizzando la c.d. tecnologia di corrispondenza dei modelli (*pattern-matching technology*)[56]. Per comprenderne il funzionamento, si immagini un monitor televisivo su cui è proiettato il video in real-time di una particolare strada cittadina o più di una, e appena qualcuno passa davanti alla telecamera, il monitor crea un quadrato digitale intorno alla sua faccia identificandone il viso. Se le informazioni personali vengono visualizzate a fianco al volto ''riquadrato'' dal sistema, vuol dire che c'è stato un abbinamento con un'impronta precompilata di quel medesimo soggetto[57]. Le telecamere utilizzate possono essere: fisse, mobili, apposte sui droni o di proprietà pubblica o privata.

Anche in questo tipo di monitoraggio, *conditio sine qua non* per il suo utilizzo, non è necessariamente un sospetto individualizzato di reato, seppur può essere usato a fini investigativi. In generale, la giustificazione legata all'uso di questi sistemi avanzati, quindi, si traduce in una forma di pubblica

---

[54]Cfr., GARVIE Clare & MOY Laura, *America Under Watch: Face Surveillance in the United States*, in *Geo. Ctr. on priv. & tech.: am. under watch*, 2019, *https:// www.americaunderwatch.com [https://perma.cc/P6RF-56EB*] (describing how various police departments use a network of surveillance cameras to conduct face surveillance).

[55]*Ibidem.*

[56]Cfr., MOZUR Paul, *Chinese Man Caught by Facial Recognition at Pop Concert*, in *BBC News*, 2018, *https://www.bbc.com/news/world-asia-china-43751276[https://perma.cc/9DFT-5H3C]; One Month, 500,000 Face Scans: How China Is Using A.I. To Profile a Minority*, in *N.Y. Times*, 2019, *https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html* [*https://perma.cc/Z9QR-PG6F*].

[57]Cfr., MOZUR Paul, *Inside China's Dystopian Dreams, A.I. Shame and Lots of Cameras*, K, 2018, *https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html [https://perma.cc/8J37-2NEK*] ("China has an estimated 200 million surveillance cameras.").

sicurezza o controllo sociale, ad esempio per identificare tutte le persone che commettono un illecito[58].

Lo stesso tipo di sorveglianza facciale generalizzata, inoltre, può essere eseguita scansionando ingenti set di dati fotografici privati o di immagini digitali private (il c.d. *data mining*). Miliardi di immagini e video vengono registrati da sistemi di terzi privati come *Facebook*, *Google*, *Instagram*, *Twitter*, *YouTube* e altre piattaforme *online* o digitali[59]. Le immagini archiviate con queste modalità possono essere acquisite dalla polizia che, studiandone la corrispondenza, potrebbe costruire appositi dossier contenenti le informazioni degli individui in una comunità[60]. Anche questo tipo di corrispondenza di sorveglianza facciale non viene usato solo per lo scopo specifico di applicazione della legge, quanto, piuttosto, per raccogliere dati sugli individui in generale[61]. Le identificazioni risultanti dall'analisi potrebbero coinvolgere il tracciamento di alcuni dettagli personali quali: la posizione (sia dai metadati che dal contesto o contenuto delle foto condivise), connessioni personali, ''Mi piace'', interessi e attività[62]. Una delle realtà delle fotografie digitali è che, per

[58]Cfr., BURT Chris, *NEC Facial Biometrics to Be Deployed for Rugby World Cup and Busiest International Airport in Japan*, in *Biometric update*, 2018, *https://www.biometricupdate.com/201811/nec-facial-biometric-to-be-deployed -for-rugby-world-cup-and-busiest-international-airport-in-japan [https://perma.cc/ VAJ9-Z236*]; GERSHGORN Dave, *Carnival Cruises, Delta, and 70 Countries Use a Facial Recognition Company You've Never Heard of*, in *Medium: One zero*, 2020, *https:// onezero.medium.com/nec-is-the-most-important-facial-recognition-company-you've-never-heard-of-12381d530510 [https://perma.cc/6BDD-E8WJ]*.

[59]Cfr., HILL Kashmir, *The Secretive Company That Might End Privacy as We Know It*, in *N.Y.. Times*, 2020, *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/G895 -W3LJ*] (describing a facial recognition app reportedly supported by three billion images from Facebook, YouTube, and other websites); PETRESCU Virgil, *Face Recognition as a Biometric Application*, in *J. Mechatronics &Rrobotics* 2019, 237-240, 3 .

[60]Cfr., BOYD Aaron, *ICE Outlines How Investigators Rely on Third-Party Facial Recognition Services*, in *Nextgo*, 2020, *https:// www.nextgov.com/emerging-tech/2020/06/ice-outlines-how-investigators-rely- third-party-facial-recognition-services/165846 [https://perma.cc/SL4J-DHUK];* KELLY Heather & LERMAN Rachel, *America Is Awash in Cameras, a Double-Edged Sword for Protesters and Police*, in *Wash. Post*, 2020, *https://www .washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters [https://perma.cc/F4GX-XDBJ*].

[61]Cfr., PATEL Faiza, LEVINSON-WALDMAN Rachel, DENUYL Sophia, and KOREH Raya, *Map: Social Media Monitoring by Police Departments, Cities, and Counties*, in *Brennan ctr. for just.*, 2019, *https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties, [https://perma.cc/ TC22-49A3*] (describing how law enforcement has used social media monitoring software to monitor protests).

[62]Cfr., MATTHEWS Richard, *How Law Enforcement Decodes Your Photos*, in *Conversation* , 2017, *http://theconversation.com/explainer-how-law-enforcement-decodes-your-photos-78828 [https://perma.cc/7RQ8-MX5C*]; GERMAIN Thomas, *How a Photo's Hidden 'Exif' Data Exposes*

una impostazione predefinita dai *social network*, riescono a codificare informazioni su luogo, ora, data, tipo di fotocamera e dettagli sul dove, quando e come è stata scattata la foto[63].Queste sono informazioni spesso inserite nei consensi della privacy che, purtroppo, per superficialità raramente vengono letti dai più.

Il secondo tipo di meccanismo di riconoscimento facciale è la tecnologia di identificazione facciale[64] investigativa che differisce dalla sorveglianza facciale generalizzata perché la polizia ne usufruisce solo quando ha sospetti fondati circa la colpevolezza di una determinata persona. La polizia, ad esempio può ritenere che un soggetto possa essere coinvolto in un determinato crimine, a causa di un'immagine della scena di un delitto (ad es. nastro di sorveglianza, video dell'*iPhone* di un testimone) o potrebbe avere la fotografia di un indagato e, quindi tentare di abbinarla a diversi set di dati fotografici della scena criminosa[65].

In altre parole, la polizia potrebbe voler confrontare l'immagine del volto di un ‘’obiettivo’’ con un *database* di altre immagini preregistrate del viso in suo possesso[66]. Questi *database* potrebbero contenere foto o informazioni circa, ad esempio, la patente di guida foto (registri della motorizzazione statale - DMV), foto segnaletiche di arresti (foto generate dalla polizia) o altri sistemi di identificazione dei sospetti più informali (ad esempio, database di bande,

---

Your Personal Information, in *Consumer reps*, 2019, https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data *[https://perma.cc/YPG7-54AS*].

[63]*Ibidem.*

[64]Cfr., 116th CONGRESS.GOV, *Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight & Reform*, 2019, 2020.

[65]Cfr., SCHUPPE Jon, *How Facial Recognition Became a Routine Policing Tool in America*, in *NBC News*, 2019, *https://www.nbcnews.com/news/us -news/how-facial-recognition-became-routine-policing-tool-america-n1004251[https://perma.cc/P3A4-KYJR*]; HARWELL Drew, *Oregon Became a Testing Ground for Amazon's Facial- Recognition Policing. But What if Rekognition Gets It Wrong?*, in *Wash. Post*, 2019, *https://www.washingtonpost.com/technology/2019/04/30/ amazons-facial-recognition-technology-is-supercharging-local-police [https:// perma.cc/LA3C-JD8K]* .

[66]Cfr., O'NEILL James, *Opinion, How Facial Recognition Makes You Safer*, in *N.Y. Times*, 2019, *https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [https://perma.cc/HDY6-FJ35]*; HILL Kashmir, *Wrongfully Accused by an Algorithm*, in *N.Y. Times*, 2020, *https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/458E-SR99*]; TORRES Ella, *Black Man Wrongfully Arrested Because of Incorrect Facial Recognition*, in *ABC news*, 2020, *https://abcnews.go.com/US/black-man-wrongfully-arrested-incorrect -facial-recognition/story?id=71425751 [https://perma.cc/JF9M-3C8E*].

fotografie di carceri, sistemi di gestione dei dati dell'accusa)[67]. In questo scenario, la polizia che ha già identificato un sospetto e desidera confermarne l'identità utilizza gli appositi set di dati fotografici esistenti per il confronto[68].

Questo tipo di processo di identificazione facciale viene utilizzato, di frequente, dall'FBI tramite partner statali o locali, in alcuni Stati.

Ad esempio, in un anno e mezzo tra il 2017 e il 2019, l'FBI ha condotto 152.500 perquisizioni sulla base di indagini delle forze dell'ordine[69]. A New York City, nel 2018, il NYPD ha condotto 7.024 perquisizioni[70]. Il Washington Post ha riferito che un piccolo dipartimento di polizia dell'Oregon ha utilizzato un software commerciale creato da Amazon per condurre ricerche investigative su larga scala[71]. Anche la polizia di Detroit, nel Michigan, ha dichiarato di utilizzare questo tipo di riconoscimento facciale per rintracciare i sospetti violenti[72].

L'identificazione facciale, tuttavia, è limitata a fotografie statiche e non si estende ai video in *streaming* o in *real time*, e viene utilizzata solo dopo la commissione di un reato, con lo scopo di scoprirne i colpevoli. Nel prossimo

---

[67]Cfr., HARMON Amy, *As Cameras Track Detroit's Residents, a Debate Ensues over Racial Bias*, in *N.Y. Times*, 2019, *https://www.nytimes.com/2019/07/08/us/ detroit-facial-recognition-cameras.html [https://perma.cc/B5L2-9MS7*] (describing a Detroit program that compares faces on video to "50 million driver's license photo- graphs and mug shots contained in a Michigan police database"); FERGUSON Andrew Guthrie, *Big Data Prosecution and Brady*, in *Ucla*, 2020,180, 185–215, 67 (describing various prosecution databases filled with photos of suspects).

[68]Cfr., SCHUPPE Jon, *How Facial Recognition Became a Routine Policing Tool in America*, in

NBC Nnews, 2019, *https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/P3A4-KYJR]*.

[69]Cfr., 116th CONGRESS.GOV, *Facial Recognition Technology (Part 1I): Ensuring Transparency in Government Use: Hearing Before the H. Comm. on Oversight & Reform*.

[70]Cfr., O'NEILL James Opinion, *How Facial Recognition Makes You Safer*, in *N.Y. Times*, 2019, *https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [https://perma.cc/HDY6-FJ35*]; HILL Kashmir, *Wrongfully Accused by an Algorithm*, in *N.Y. Times*, 2020, *https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/458E-SR99*].

[71]Cfr., HARWELL Drew, *Oregon Became a Testing Ground for Amazon's Facial- Recognition Policing. But What if Rekognition Gets It Wrong?*, in *Wash. post*, 2019, *https://www.washingtonpost.com/technology/2019/04/30/ amazons-facial-recognition-technology-is-supercharging-local-police [https:// perma.cc/LA3C-JD8K*] (describing how police departments use facial-recognition algorithms to search through hundreds of thousands of images to find a match).

[72]Cfr., HARMON Amy, *As Cameras Track Detroit's Residents, a Debate Ensues over Racial Bias*, in *N.Y. Times*, 2019, *https://www.nytimes.com/2019/07/08/us/ detroit-facial-recognition-cameras.html [https://perma.cc/B5L2-9MS7]*.

futuro questo tipo di corrispondenza del database potrebbe essere esteso anche a situazioni quali sospetti di reato o, banalmente, in contesti quali il blocco del traffico da parte della polizia per controlli a ''campione''[73]. L'evoluzione di questi nuovi sistemi identificativi è sempre più elevata, al punto che alcune società private stanno già vendendo programmi volti ad eseguire la ricerca su un semplice telefono cellulare[74]. Sarebbe utile, infatti, ottenere, in questo modo, la capacità di identificare rapidamente qualcuno da una sua foto sul telefono[75].

Una delle più importanti società private è *Clearview AI*, che ha salvato e classificato miliardi di immagini di volti da siti Internet e dai *social media* e ha creato il proprio *database* per l'ausilio delle forze dell'ordine[76]. *Clearview AI* ha, così, stipulato collaborazioni con centinaia di forze dell'ordine e dipartimenti di polizia locali e condotto ricerche di riconoscimento facciale per identificare i sospetti[77]. Il sistema *Clearview*, tuttavia, a causa del fatto che prelevava le immagini altrui, ledendo la loro privacy e le registrava nel suo database, principalmente da siti come *Twitter*, violando le loro politiche, le pratiche dell'azienda sono state sottoposte a cause legali circa il sospetto della loro dubbia legalità, pur non essendo l'unica azienda a vendere informazioni

---

[73]Cfr., DELLA CAVA Marco, *California Could Become First to Limit Facial Recognition Technology; Police Aren't Happy*, in *USA Today*, 2019, *https:// www.usatoday.com/story/news/nation/2019/06/16/california-could-limit-how-police-use-facial-recognition-technology/1456448001 [https://perma.cc/9AZS-8P5F*] ("State law enforcement officials here do not now employ the technology [facial recognition in body cameras] . . . But some police officials oppose the bill on the grounds that a valuable tool could be lost.").

[74]Cfr., FACEFIRST, *http://web.archive.org/web/20200620203318/https://www.facefirst.com/industry/law-enforcement-face-recognition*.

[75]Cfr., HARWELL Drew, *Oregon Became a Testing Ground for Amazon's Facial- Recognition Policing. But What if Rekognition Gets It Wrong?*, in *Wash. post*, 2019, *https://www.washingtonpost.com/technology/2019/04/30/ amazons-facial-recognition-technology-is-supercharging-local-police [https:// perma.cc/LA3C-JD8K]*.

[76]Cfr., FRIED Ina, *Clearview Brings Privacy Concerns from Facial Recognition into Focus*, in *Axios*, 2020, *https://www.axios.com/clearview -facial-recognition-law-enforcement-ac069290-b83e-4934-a9f0-0b782af82588.html [https://perma.cc/X4S6-QJFG];* HILL Kashmir, *The Secretive Company That Might End Privacy as We Know It*, in *N.Y. Times*, 2020, *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, [https://perma.cc/G895 -W3LJ*].

[77]ID., Cfr., REICHERT Corinne, *Clearview AI Is Looking to Expand Globally, Report Says*, in *CNET*, 2020, *https://www.cnet.com/news/clearview-ai-reportedly-looking-to-expand-globally [https://perma .cc/4UXM-6SRH*] (reporting that the company wants to sell its technology to law enforcement in Australia, Dubai, Sweden, Nigeria, and other countries).

concernenti il riconoscimento facciale alle forze dell'ordine[78].Nonostante tali questioni, la ricerca di volti nel database *Clearview* era semplice come usare Google, quindi è risultato un sistema davvero utile, veloce ed efficace[79].

La terza forma di riconoscimento facciale è il c.d. *"Face tracking"* (il tracciamento del volto), un termine che si usa per descrivere un ibrido tra la sorveglianza facciale e l'identificazione del volto, dato che coinvolge le medesime tecnologie di sorveglianza del volto c.d. ‘’video generalizzato’’ ma il tracciamento inizia solo se alla base sussiste un sospetto particolare in capo ad un soggetto[80].

La polizia quindi ‘’traccia’’ quando sono in corso attivamente le indagini per la commissione, già avvenuta, di un determinato crimine. Il sospetto, in capo ad un individuo in particolare, nasce dal *matching*, ad esempio della scena del crimine, riconosciuto da un software di riconoscimento facciale[81]. La polizia può utilizzare la tecnologia del *"face tracking"* in tre modi diversi: (i) scansionare i filmati archiviati per identificare un volto preso di mira in mezzo ad una folla[82]; (ii) scansione di *feed* video in tempo reale per identificare un volto preso di mira[83]; e (iii) scansione di database di immagini da piattaforme private di terze parti per identificare un determinato volto (*data mining*)[84].

---

[78]Cfr., RIVERO Nicolás, *The Little-Known AI Firms Whose Facial Recognition Tech Led to a False Arrest*, in *Quartz*, 2020, *https://qz.com/1873731/the-unknown -firms-whose-facial-recognition-led-to-a-false-arrest [https://perma.cc/8MMN -H9V6*] (describing the companies that developed and sold the facial recognition technology that Detroit police used when they arrested an innocent man).

[79]Cfr., MATSAKIS Louise, *Scraping the Web Is a Powerful Tool. Clearview AI Abused It*, in *Wired*, 2020, *https://www.wired.com/story/clearview-ai-scraping-web[https://perma.cc/7VTF-KS66*]; PEREZ Gisela & COOK Hilary, *Google, YouTube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App that Helps Law Enforcement*, in *CBS News*, 2020, *https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial -recognition-app [https://perma.cc/UE64-UZBA*]; PORTER Jon, *Facebook and LinkedIn Are Latest to Demand Clearview Stop Scraping Images for Facial Recognition Tech*, in *Verge*, 2020, *https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter -youtube , [https://perma.cc/AX4H-A9BJ]*.

[80]Cfr., FERGUSON Andrew Guthrie, *Facial Recognition and the Fourth Amendment*, 2019, in *Minnesota Law Review*, 2021, 1105, 105, Available at SSRN: *https://ssrn.com/abstract=3473423* or *http://dx.doi.org/10.2139/ssrn.3473423* , 118.

[81]*Ibidem.*

[82]*Ibidem.*

[83]*Ibidem.*

[84]*Ibidem.*

Per il primo tipo di *''face tracking''*, ossia il tracciamento mediante filmati archiviatio reti di *feed* video, si intende l'analisi della polizia, dopo la commissione di un crimine, della videosorveglianza cittadina memorizzata, per confrontare l'immagine del volto ''ricercato''[85], tentando di trovare qualche riscontro[86].

La ricerca di corrispondenze, all'interno di riprese video archiviate da una rete di telecamere, potrebbe, ad esempio, rivelare gli spostamenti del "bersaglio" nel tempo, inclusi ora, data, luogo, e modelli di movimento[87]. Ai luoghi, inoltre, sono spesso correlate altre informazioni quali gli interessi, relativamente ai locali frequentati, l'occupazione, il culto e la religione, gli eventuali problemi di salute, procedimenti pendenti o questioni legali in generale[88]. Il mosaico delle attività della persona, connesse mediante lo studio dei *big data*, tecniche di mappatura, e screening della personalità, potrebbe essere talmente preciso da rivelare o prevedere la posizione del soggetto identificato dal *face tracking* in tempo reale.

Come discusso in precedenza, anche la tecnologia della sorveglianza facciale viene applicata ai filmati archiviati, ma c'è una importante differenza rispetto al tracciamento del volto tramite video registrati: lo scopo. In altre parole, seppur le metodologie scientifiche utilizzate sono molto simili, ciò che differisce completamente sono i motivi alla base della scansione del viso. Infatti, la sorveglianza nasce come mero strumento di controllo generalizzato, volto a garantire la pubblica sicurezza; invece, il tracciamento viene utilizzato solo ed esclusivamente dopo la commissione di un reato per trovarne il responsabile, è quindi un vero e proprio strumento investigativo individualizzato o c.d. ''particolarizzato''[89].In parole semplici, la sorveglianza

---

[85]Cfr., GARVIE Clare & MOY Laura, *America Under Watch: Face Surveillance in the United States*, in *Geo. ctr. on priv. & tech.: am. under watch*, 2019, *https:// www.americaunderwatch.com [https://perma.cc/P6RF-56EB*] (describing how various police departments use a network of surveillance cameras to conduct face surveillance).

[86]*Ibidem.*

[87]*Ibidem.*

[88]*Ibidem.*

[89]Cfr., FERGUSON Andrew Guthrie, *Facial Recognition and the Fourth Amendment*, 2019, in *Minnesota Law Review*, 2021, 1105, 105, *https://ssrn.com/abstract=3473423* or *http://dx.doi.org/10.2139/ssrn.3473423* , 118.

mira all'identificazione di tutti, il tracciamento ricerca un volto specifico. È evidente, tuttavia, che il pericolo legato all'uso di queste tecnologie facciali, in generale, resta il medesimo: quello di una diffusa sorveglianza di massa indiscriminata, fortemente lesiva della privacy.

Il secondo tipo di *face tracking*, invece, consiste nell'uso di ''sistemi video in rete'' per tracciare i sospetti in tempo reale[90]. Un ''sistema in rete'' di tracciamento dei volti in *real-time* è in grado, potenzialmente, di fornire la posizione specifica di un "ricercato" appena ''trovato''[91]. La corrispondenza (*match*) o il c.d. "colpo" fa scattare un avviso, indirizzato alla polizia, circa la posizione, in tempo reale dell'obiettivo, da identificare nella città[92].

Nel gennaio del 2020, la *London Metropolitan Police* ha implementato l'azione investigativa utilizzando uno strumento di sorveglianza del riconoscimento facciale in grado di abbinare i volti, in *real time*, a quelli presenti in una "lista di controllo" memorizzata nei *database* delle forze dell'ordine[93]. Questo tipo di corrispondenza, teoricamente, funzionerebbe anche con l'ausilio di mere macchine fotografiche, o di singole telecamere o un singolo drone volti ad individuare una determinata persona in un determinato luogo sulla base di una corrispondenza di riconoscimento facciale derivante da un set di dati precompilato, non essendo quindi necessario, in questo caso, l'uso necessario di ingenti quantità di telecamere.

---

[90]Cfr., GARVIE Clare & MOY Laura, *America Under Watch: Face Surveillance in the United States*, in *Geo. ctr. on priv. & tech.: am. under watch*, 2019, *https:// www.americaunderwatch.com [https://perma.cc/P6RF-56EB*] (*describing how various police departments use a network of surveillance cameras to conduct face surveillance*).

[91]ID.; Cfr., HARMON Amy, *As Cameras Track Detroit's Residents, a Debate Ensues over Racial Bias*, in *N.Y. Times*, 2019, *https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html [https://perma.cc/B5L2-9MS7*].

[92]V., *Police Unlock AI's Potential To Monitor, Surveil and Solve Crimes*, in *Wall St. J. Video*, 2019, *https://www.wsj.com/video/police-unlock-ai-potential-to-monitor-surveil-and-solve-crimes/819D5F78-22BC-4A41-9517AE31BE3C5E7E.html* [*https://perma.cc/HX8A-ZJ5J*] (*showing how police departments employ face-recognition technology*).

[93]Cfr., LOMAS Natasha, *London's Met Police Switches on Live Facial Recognition, Flying in the Face of Human Rights Concerns*, in *Techcrunch*, 2020, *https:// techcrunch.com/2020/01/24/londons-met-police-switches-on-live-facia -recognition-flying-in-face-of-human-rights-concerns* [*https://perma.cc/Y9QR-L7E6*]; DOUGLAS Jason & OLSON Parmy, *London Police to Start Using Facial Recognition Cameras*, in *Wall St.J.*, 2020, *https://www.wsj.com/articles/london-police-to-start-using-facial-recognition-cameras-11579895367* [*https://perma.cc/ A3AZ-DARA*].

Il terzo tipo di tracciamento riguarda l'uso di immagini di volti registrate da fornitori privati, quindi posseduti da terze parti, che ''vendono'' questi dati alla polizia che può utilizzarli, ricercando dei loro database, per trovare un riscontro con un sospettato. La tecnologia usata in questi casi è simile a quella di ''corrispondenza dei modelli''[94].L'accesso della polizia a questi *set* di dati, che è reso possibile tramite una richiesta informale, citazione in giudizio, mandato o acquisto, può aiutarla a identificare indagati, gruppi delinquenziali, e associati criminali[95]. Questi *dataset* di foto, possedute da terze parti, non solo aiutano le forze dell'ordine nel processo di identificazione facciale, ma rivelano anche dati sulla posizione tramite i metadati raccolti che tracciano dove e quando le foto sono state scattate e con quale dispositivo e tipo di telecamera[96]. Sebbene spesso un singolo dato non aiuti il procedimento investigativo, queste informazioni, riguardanti la posizione, se ''aggregate'' e tracciate sul lungo termine potrebbero essere rivelatrici, tramite deduzioni fotografiche, di interessi, percorsi, luoghi frequentati e altro, fino a stimare dove è probabile che il sospettato si recherà nel futuro.

La polizia sta già usufruendo di questi sistemi, monitorando, ad esempio, i social media per il controllo della violenza e delle minacce delle bande criminali. In sostanza le azioni di polizia si proiettano, sempre di più, verso il ''controllo di tutti'', e per quanto questo possa essere utile per la prevenzione del crimine e per la maggiore celerità delle indagini e dei processi, l'indiscriminata lesione della sfera personale degli individui sembra permanere come questione irrisolta[97].

---

[94]Cfr., Facebook users alone upload 350 million photos per day. ASLAM Salman, *Facebook by the Numbers: Stats, Demographics & Fun Facts*, in *Omnicore*, 2020, *https://www.omnicoreagency.com/facebook-statistics* [*https://perma.cc/936W -4Z9G*].

[95]Cfr., O'NEILL James Opinion, *How Facial Recognition Makes You Safer*, in *N.Y. Times*, 2019, *https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [https://perma.cc/HDY6-FJ35*].

[96]Cfr., MATTHEWS Richard, *How Law Enforcement Decodes Your Photos*, in *Conversation*, 2017, *http://theconversation.com/explainer-how-law-enforcement-decodes-your-photos-78828* [*https://perma.cc/7RQ8-MX5C*]; GERMAIN Thomas, *How a Photo's Hidden 'Exif' Data Exposes Your Personal Information*, in *Consumer Reps*, 2019, *https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data* [*https://perma.cc/YPG7-54AS*].

[97]Cfr., AUSTEN Ben, *Public Enemies: Social Media Is Fueling Gang Wars in Chicago*, in *Wired*, 2013, *https://www.wired.com/2013/09/gangs-of-social-media* [*https:// perma.cc/MD29-DC4N*]

Sulla base di quanto esplicato, analizzando, in generale, le quattro tecnologie facciali è possibile evincere, conclusivamente, i pro e contro delle singole fattispecie.

In primis la ''verifica facciale'' risulta la più accurata, grazie al sistema binario utilizzato per confermare l'identità, usando come riscontro le foto di passaporti o carte di identità[98]. D'altra parte, il sistema di identificazione del volto ricerca tra migliaia (o milioni) di immagini e riesce a trovare la migliore corrispondenza possibile, prendendo in considerazione aspetti come gli angoli, prospettive e illuminazione del viso[99]. Da ultimo, la sorveglianza e il rilevamento del volto sono i più complessi, a causa del fatto che le tecniche di riscontro sono applicate in tempo reale e attraverso l'analisi di vasti flussi di immagini digitali. Questo meccanismo è, spesso, di difficile applicazione dato che la sorveglianza *real-time* su larga scala causa maggiori possibilità di errore[100].

Per un corretto funzionamento, il riconoscimento facciale, in generale, necessita di almeno due c.d. ''*set*'' di immagini[101]: una raccolta di immagini di volti o foto segnaletiche digitalizzate e un secondo set di dati digitali che servono per confrontare quelle impronte facciali (che derivano ad es. su immagini fisse o flussi video in diretta o archiviati (ad esempio, telecamere di

(explaining how police monitor social media to anticipate and respond to crimes); GOLDSTEIN Joseph & GOODMAN J. David, *Seeking Clues to Gangs and Crime, Detectives Monitor Internet Rap Videos*, in *N.Y. Times*, 2014, https://www.nytimes.com/2014/01/08/nyregion/seeking-clues-to-gangs-and-crime-detectives-monitor-internet-rap-videos.html, [*https://perma.cc/E2FC-XYN9*] .

[98]Cfr., ULLAH Eisa Anis Ishrat & KHANUMM Akheela, *A Comparative Study of Facial Recognition Systems*, in *Int'l J. Advanced rsch. comput. sci.* , (special issue no. 2), 2018 ,114, 114 , 9.

[99]Cfr., LEVASHOV Kirill, *The Rise of a New Type of Surveillance for Which the Law Wasn't Ready*, in *Colum. Sci. & Tech.*, 2013, 15, 169, (stating that "[e]ven slight changes, like adding makeup," can make finding a match difficult).

[100]Cfr., ULLAH Eisa Anis Ishrat & KHANUMM Akheela, *A Comparative Study of Facial Recognition Systems*, in *Int'l J. Advanced rsch. comput. sci.* , (special issue no. 2), 2018 ,114, 114 , 9.("*A facial recognition algorithm has its focus on two main tasks i.e. recognition and verification with verification being much more easier as compared to recognition, as verification does a kind of binary mapping by verifying the input image which is already present in the database."*).

[101]Cfr., Cfr., BUOLAMWINI JOY, ORDÓÑEZ VICENTE, MORGENSTERN JAMIE & LEARNED ERIK MILLER, *Facial recognition technologies: a primer*, 2020, 8 e 13, https://global-uploads.webflow.com/5e027cal88c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf *[https://perma.cc/X8CH-JAV3]*.

sorveglianza, telecamere indossate dalla polizia, telecamere di sorveglianza private, quindi un'ampia varietà di *settings*[102]) e ottenere un riscontro[103].

3. Problematiche relative a errore, pregiudizio, equità, trasparenza legato all'uso dell'IA

Nei campi dell'informatica e dell'analisi dei dati, l'uso etico dell'intelligenza artificiale è ora un argomento di conversazione seria[104]. Emergono questioni problematiche relative alla possibilità di errori, da parte di questi sistemi, problemi di scarsa imparzialità o equità e trasparenza. Per colmare questi *gap*, si mira sempre di più a costruire tecnologie di riconoscimento facciale "migliori"[105], ma sussistono ad oggi numerose problematiche, soprattutto correlate al fatto che queste macchine intelligenti, seppur mediamente autonome, restano spesso legate ai pregiudizi ed errori umani eventualmente presenti nel linguaggio di programmazione, causando incertezze applicative[106].

Il filo conduttore di queste critiche è legato al fatto che l'obiettività derivante dal codice e dai modelli informatici può essere distorta da qualsiasi interazione umana[107]. Tuttavia, anche senza alcun tipo supervisione umana, i sistemi di

---

[102]Cfr., *Police Unlock AI's Potential To Monitor, Surveil and Solve Crimes*, in *wall st. j. Video*, 2019, https://www.wsj.com/video/police-unlock-ai -potential-to-monitor-surveil-and-solve-crimes/819D5F78-22BC-4A41-9517AE31BE3C5E7E.html [*https://perma.cc/HX8A-ZJ5J*] (showing how police departments employ face-recognition technology).

[103]*Ibidem.*

[104]Cfr., ACM FACCT, *Ass'n for computing mach. conf. on fairness, accountability & transparency*, *https://facctconference.org/index.html [https://perma.cc/ 5WLQ-DS86*]; BAROCAS Solon & SELBST Andrew D., *Big Data's Disparate Impact*, in *Calif.*, 2016, 671, 683–684, 104, ("Because data mining relies on as ground truth, when those inputs are themselves skewed by bias or inattention, the resulting system will produce results that are at best unreliable and at worst discriminatory.").

[105]*Ibidem.*; IVANOVA Irina, *Why Face-Recognition Technology Has a Bias Problem*, in *CBS news*, 2020, *https://www.cbsnews.com/news/facial-recognition-systems-racism-protests-police-bias [https:// perma.cc/Q7ZU-4R33*].

[106]Cfr., PASQUALE FRANK, *The black box society 18*, 2015; BUOLAMWINI Joy, *How I'm Fighting Bias in Algorithms*, in *Ted*, 2016, *https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms* [*https://perma.cc/32RE-CAYQ*]; O'NEIL CATHY, *Weapons of math destruction: how big data increases inequality and threatens democracy*, 2016, (discussing how bias that is written into algorithms has far-reaching, negative consequences); NOBLE SAFIYAUMOJA, *Algorithms of oppression: how search engines reinforce racism*, 2018, (discussing how search engine algorithms perpetuate bias by producing stereotypical, offensive, and stigmatizing results); EUBANKS VIRGINIA, *Auto- mating inequality 37*, 2018.

[107]Cfr., CITRON Danielle Keats & PASQUALE Frank A., *The Scored Society: Due Process for Automated Predictions*, in *Wash*, 2014, 1, 89, (discussing how data ranking creates stigmatization in

intelligenza artificiale potrebbero, allo stesso modo, reificare i pregiudizi strutturali esistenti, pur essendo, al contempo, basati tendenzialmente su dati (*data-driven based*), di natura neutra e obiettiva[108]. Nel caso specifico del *facial recognition*, le questioni diventano sempre più complesse[109].

Innanzitutto, la sorveglianza facciale non sempre funziona come previsto. Sono state dimostrate reali preoccupazioni circa l'accuratezza delle corrispondenze del volto[110]. I primi *test* di riconoscimento facciale, in particolare di sorveglianza, su larga scala hanno avuto scari risultati, rasentando tassi di errori elevatissimi[111].Tuttavia, anche in ambienti più ristretti, si sono verificati, seppur in minor percentuale, errori che hanno condotto a false corrispondenze.

AI scoring systems); RUHA BENJAMIN, *Race after technology: abolitionist tools for the new jim code* , 2019, 112 s. (discussing misguided use of electronic surveillance by private companies in the movement for decarceration); OHM Paul, *The Underwhelming Benefits of Big Data*, in *U. Pa.*, 2012, 339-340, 161, *https://www.pennlawreview.com/wp-content/uploads/2020/05/161-U-Pa -L-Rev-Online-339.pdf* [*https://perma.cc/U3FS-B9M8*]

[108]Cfr., CRAWFORD Kate & SCHULTZ Jason, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, in *B.C.*, 2014, 93-94, 55 , ("Personal harms emerge from the inappropriate inclusion and predictive analysis of an individual's personal data without their knowledge or express consent."); JOH Elizabeth E., *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, in HARV. L. & POL'Y, 2016, 10, 115-116, 15. ; SELBST Andrew D., *Disparate Impact in Big Data Policing*, in *GA.*, 2017, 109-113,52; BRAYNE Sarah, *The Criminal Law and Law Enforcement Implications of Big Data*, in *Ann. rev. l. & Soc. sci.* , 2018, 293-294, 14; *c.f* KALLURI Pratyusha, *Don't Ask If Artificial Intelligence Is Good or Fair, Ask How It Shifts Power*, in *Na-ture*, 2020, *https://www.nature.com/articles/d41586-020-02003-2* [*https://perma.cc/N9MY-M8G9*]

[109]Cfr., WOODWARD John D., *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, in *U. Pitt.*, 1997, 97, 134, 59; CLARKE Roger, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, in *Info. Tech. & people*, 1994, 6, 34, 7; v. anche DEVICH Malkia -Cyril, *Defund Facial Recognition*, in *Atlantic*, 2020, *https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771[https://perma.cc/9P29-JD63];* v. LEARNED-MILLER ERIK, ORDÓÑEZ VICENTE, MORGENSTERN JAMIE & BUOLAMWINI JOY, *Facial recognition technologies in the wild: a call for a federal office*, 2020, 3 s., *https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/ 5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf* [*https://perma.cc/ 5BGG-ML6V*].

[110]Cfr., GARVIE Clare & MOY Laura, *America Under Watch: Face Surveillance in the United States*, in *Geo. ctr. on priv. & tech.: am. under watch*, 2019, *https:// www.americaunderwatch.com* [*https://perma.cc/P6RF-56EB*] (describing how various police departments use a network of surveillance cameras to conduct face surveillance); v. BUOLAMWINI JOY, ORDÓÑEZ VICENTE, MORGENSTERN JAMIE & LEARNED ERIK -MILLER, *Facial recognition technologies: a primer* , 2020, 14 e 16 , *https://global-uploads.webflow.com/5e027cal88c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf*, [*https://perma.cc/X8CH-JAV3*].

[111]Cfr., JEE Charlotte, *London Police's Face Recognition System Gets It Wrong 81% of the Time*, in *Mit Tech. rev.*, 2019, *https://www.technologyreview.com/2019 07/04/134296/london-polices-face-recognition-system-gets-it-wrong-81-of-the -time*, [*https://perma.cc/X4J6-TL3V*].

Un celebre esempio è quello legato al test effettuato tramite l'analisi di un software di identificazione facciale disponibile in commercio che ha condotto alla erronea identificazione dei ventotto membri del Congresso degli Stati Uniti, che sono stati falsamente abbinati alle foto segnaletiche di alcuni[112]. Anche il *National Institute of Standards and Technology* (*NIST*) ha riscontrato errori significativi derivanti da esperimenti, effettuati dai fornitori di sistemi di riconoscimento facciale[113], soprattutto nell'identificare le donne di colore[114]. I problemi sono legati sia a fattori intrinseci che estrinseci, comprese le modalità in cui le foto vengono ''catturate'' e registrate sia la complessità dei lineamenti del viso e del movimento facciale umano[115]. Questo problema di errore, o per meglio dire, di precisione, tuttavia, potrebbe risolversi presto poiché i miglioramenti nella corrispondenza basata sui modelli di acquisizione dei *big data* consentiranno, sempre di più, alle aziende di migliorare i propri tassi di accuratezza nel tempo[116].

Tuttavia, è da considerare che l'errore legato al *matching* di identità ha conseguenze davvero rilevanti, poiché una corrispondenza sbagliata o imprecisa può condurre a risultati investigativi fuorvianti, cagionando

---

[112]Cfr., SNOW Jacob, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, in *Aclu*, 2018, *https://www.aclu.org/blog/privacytechnology/surveillance-technologies/amazons-face-recognition-falsely -matched-28* [*https://perma.cc/9JS3-6TRM*].

[113]Cfr., GROTHER PATRICK, NGAN MEI & HANAOKA KAYEE, *Nat'l inst. standards & tech., internal rep. 8280, face recognition vendor test (frvt) part 3: demographic effects*, 2019, 2 s., *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf*, [*https://perma.cc/4VEW-SD7F*]; BUSHWICK Sophie, *How NIST Tested Facial Recognition Algorithms for Racial Bias*, in *Sci. Am.*, 2019, *https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias* [*https://perma.cc/9JFT-GV22*] *("NIST's tests revealed that many of these algorithms were 10 to 100 times more likely to inaccurately identify a photograph of a black or East Asian face, compared with a white one. In searching a database to find a given face, most of them picked incorrect images among black women at significantly higher rates than they did among other demographics.").*

[114]*Ibidem.* GROTHER et al, 63; v. anche HARWELL Drew, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, in *Wash. Post*, 2019, *https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use, [https://perma.cc/8967-B8VM]*.

[115]Cfr., JOSHI Jagdish Chandra & GUPTA K.K., *Face Recognition Technology: A Review*, in *Iup J. Telecomms* , 2016, 8, 59, (recognizing intrapersonal problems such as "age, facial expression and facial details/equipment used (*facial hair, glasses, cosmetics, veil, etc*.)" e estrinsecano questioni come: "*illumination, pose, scale and imaging parameters'' (e.g., resolution, focus, imaging, noise, etc.)" as causing a myriad of challenges in algorithmic recognition techniques*).

[116]Cfr., SIMONITE Tom, *The Best Algorithms Struggle to Recognize Black Faces Equally*, in *Wired*, 2019, *https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally* [*https://perma.cc/H8KP-AGPC*].

potenzialmente, nella peggiore delle ipotesi, ad arresti e azioni penali in capo ad un indagato-imputato-condannato diverso rispetto a quello realmente responsabile. Il pericolo di riscontri c.d. ''falsi positivi'' porta, quindi, a falsi arresti[117], e, di conseguenza, ad un erroneo uso coercitivo da parte della polizia[118]. In un contesto futuro di uso frequente della tecnologia della sorveglianza facciale, che opera con decine di migliaia di volti scansionati ogni giorno, una corrispondenza imprecisa potrebbe creare, se non sanata, notevoli problemi applicativi[119].

Durante le azioni di polizia, infatti, può essere difficile per un singolo agente ignorare il sospetto dell'algoritmo, conducendolo ad effettuare alcune fermate o controlli errati e/o a trascurare elementi rilevanti ai fini investigativi[120].

---

[117]Cfr., HILL Kashmir, *The Secretive Company That Might End Privacy as We Know It*, in *N.Y. Times*, 2020, *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html*, [*https://perma.cc/G895 -W3LJ*] (*describing a facial recognition app reportedly supported by three billion images from Facebook, YouTube, and other websites*); HILL Kashmir, *Wrongfully Accused by an Algorithm*, in *N.Y. Times*, 2020, *https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html* [*https://perma.cc/458E-SR99*]; TORRES Ella, *Black Man Wrongfully Arrested Because of Incorrect Facial Recognition*, in *ABC News*, 2020, *https://abcnews.go.com/US/black-man-wrongfully-arrested-incorrect -facial-recognition/story?id=71425751, [https://perma.cc/JF9M-3C8E*]; HOLT Kris, *Facial Recognition Linked to a Second Wrongful Arrest by Detroit Police*, in *Engadget*, 2020, *https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.htm,l [https://perma.cc/KS46-YWGW]*.

[118]Cfr., FOX Jeremy C., *Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect*, in *Bos. Globe*, 2019, *https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html*, *[https:// perma.cc/RZK4-WVXD*] *(describing the emotional distress of receiving death threats and calls for death of mistaken identity victim)*; *cf.* WILLIAMS Robert, *Opinion, I Was Wrongfully Arrested Because of Facial Recognition. Why Are Police Allowed to Use It?*, in *Wash. post*, 2020, *https:// www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology*, *[https://perma.cc/XRD7-JFVR*] *(describing an innocent man's experience of being arrested for a non-violent crime based on Detroit police's use of facial recognition technology)*.

[119]Cfr., BUOLAMWINI Joy, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, in *Time*, 2019, *http://time.com/5520558/ artificial-intelligence-racial-gender-bias, [https://perma.cc/9USJ-K94C*]; CUSHING Tim, *Detroit Police Chief Says Facial Recognition Software Involved in Bogus Arrest Is Wrong '96 Percent of the Time*, in *Techdirt*, 2020, *https://www.techdirt.com/articles/20200629/17423944814/detroit-police-chief-says-facial-recognition-software-involved-bogus-arrest-is-wrong-96-percent-time.shtml [https://perma.cc/9FC8-H2QU*]; LEE Timothy B., *Detroit Police Chief Cops to 96-Percent Facial Recognition Error Rate*, in *Arstechnica*, 2020, *https://arstechnica.com/tech-policy/2020/06/detroit-police-chief-admits-facial-recognition-is-wrong-96-of-the-time, [https://perma.cc/DX2G-986E*].

[120]Cfr., HILL Kashmir, *The Secretive Company That Might End Privacy as We Know It*, in *N.Y. Times*, 2020, *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, [https://perma.cc/G895 -W3LJ*]; HILL Kashmir, *Wrongfully Accused by an Algorithm*, in *N.Y. Times*, 2020, *https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html, [https://perma.cc/458E-SR99*]; HOLT Kris, *Facial Recognition Linked to a*

In secondo luogo, ci sono problemi di mancata imparzialità e disuguaglianze strutturali che ‘’infettano’’ i dati utilizzati nei modelli di riconoscimento facciale[121].

La ‘’parzialità’’ è in parte legata al fatto che i sistemi di riconoscimento facciale sono stati inizialmente progettati per identificare popolazioni ‘’omogenee’’ di uomini bianchi, e con il compito di riconoscere i volti di altre razze[122], soprattutto uomini o donne di colore[123], e individui aventi caratteristiche ‘’particolari’’ (es. persone con capelli rossi, albini, persone che soffrono di patologie malformative…), ‘’non conformi ai canoni c.d.

Second Wrongful Arrest by Detroit Police, in *Engadget*, 2020, *https:// www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.html, [https://perma.cc/KS46-YWGW*]; TORRES Ella, *Black Man Wrongfully Arrested Because of Incorrect Facial Recognition*, in *ABC News*, 2020, *https://abcnews.go.com/US/black-man-wrongfully-arrested-incorrect-facial-recognition/story?id=71425751, [https://perma.cc/JF9M-3C8E*].

[121]Cfr., BUOLAMWINI Joy, *How I’m Fighting Bias in Algo- rithms*, in *Ted*, 2016, *https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms [https://perma.cc/32RE-CAYQ*]; BOULAMWINI Joy, *Opinion, When the Robot Doesn’t See Dark Skin*, in *N.Y. Times*, 2018, *https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html [https://perma.cc/UV8U-YV93*] *(“A.I. systems are shaped by the priorities and prejudices—conscious and unconscious—of the people who design them . . . ”)*; BENJAMIN RUHA, *Race after technology: abolitionist tools for the new jim code* , 2019, 109; CHINOY Sahil, Opinion, *The Racist History Behind Facial Recognition*, in *N.Y. times*, 2019, *https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html, [https://perma.cc/DP34-4MWR*].

[122]Cfr., BUOLAMWINI Joy, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here’s How to Solve It*, in *Time* , 2019, *http://time.com/5520558/ artificial-intelligence-racial-gender-bias, [https://perma.cc/9USJ-K94C*]; SIMONITE Tom, *Photo Algorithms ID White Men Fine—Black Women, Not So Much*, in *Wired*, 2018, *https://www.wired.com/story/ photo-algorithms-id-white-men-fineblack-women-not-so-much, [https://perma.cc/ M5CM-JNXR*]; SIMONITE Tom, *The Best Algorithms Struggle to Recognize Black Faces Equally*, in *Wired*, , 2019, *https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally , [https://perma.cc/H8KP-AGPC*].

[123]Cfr., BUOLAMWINI Joy, *When AI Fails on Oprah, Serena Williams, and Michelle Obama, It’s Time to Face the Truth*, in *Medium*, 2018, *https://medium.com/@Joy .Buolamwini/when-ai-fails-on-oprah-serena-williams-and-michelle-obama-its-time-to-face-truth-bf7c2c8a4119, [https://perma.cc/AQC8-PQES*] *(“Error rates were as high as 35% for darker-skinned women . . . ”)*; BUOLAMWINI Joy & GEBRU Timnit, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proc. Mach. Learning Rsch*, 2018, 1,11, 81, *http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, [https://perma.cc/Z2XX-GSB3*].

ordinari[124]. Il pregiudizio sistemico presente nei *dataset*[125], correlato ai dati incompleti, errati o frammentari[126], conduce, inevitabilmente, ad un sistema che discrimina chiunque tranne gli uomini bianchi e cancella, quasi completamente, la categoria dei transgender, degli individui con identità non binarie (*non-binary people*)[127].

Poiché il pregiudizio è legato ad elementi quali la razza e il genere, gli errori o le imprecisioni potrebbero seguire i medesimi schemi[128]. In alcuni casi, ciò si tradurrà nel fatto che le persone con la pelle più scura non saranno rilevate dal sistema o le corrispondenze saranno maggiormente imprecise[129].

In terzo luogo, sussistono problemi applicativi legati all'equità. Ci si domanda se sia adeguato o corretto usufruire di un sistema di riconoscimento facciale, basato sui tratti dell'uomo ''bianco'' su una popolazione diversificata.

---

[124]Cfr., FERGUSON Andrew Guthrie, *Facial Recognition and the Fourth Amendment*, 2019, in *Minnesota Law Review* , 2021, 1105, 105, Available at SSRN: *https://ssrn.com/abstract=3473423* or *http://dx.doi.org/10.2139/ssrn.3473423*, 162.

[124]Cfr., MCCLURG AJ, "*In the Face of Danger: Facial Recognition and the Limits of Privacy Law*.", in *Harvard Law Review*, vol. CXX, no. 7, 2007, 1870 e 1891., *http://www.jstor.org/stable/40042639*; cfr., COOK Cynthia M., HOWARD John J., SIROTIN Yevgeniy B., TIPTON Jerry L. & VEMURY Arun R., *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, in INST. ELEC. & ELEC. ENG'RS TRANSACTIONS ON BIOMETRICS, BEHAV. & IDENTITY SCI. (a cura di), 2019, *https:// ieeexplore.ieee.org/document/8636231 [https://perma.cc/5HB5-HAT2*].

[125]Cfr., MERLER MICHELE, RATHAN ALINI, FERIS ROGERIO & SMITH JOHN R., *Ibmrsch., diversity in faces*, 2019, 4, *https://arxiv.org/pdf/1901.10436.pdf, [https://perma.cc/ Z5BU-XXP9*] *("Face recognition systems that are trained within only a narrow context of a specific data set will inevitably acquire bias that skews learning towards the specific characteristics of the dataset.").*

[126]Cfr., GARVIE Clare & MOY Laura, *America Under Watch: Face Surveillance in the United States*, in *Geo. ctr. on priv. & tech.: am. under watch*, 2019, *https:// www.americaunderwatch.com, [https://perma.cc/P6RF-56EB]*.

[127]Cfr., 116th CONGRESS.GOV, *Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight & Reform*, 2019, 2020, 15 (statement of BUOLAMWINI Joy, Founder, *Algorithmic Justice League*); ALKHATIB Ali et al., *On Recent Research Auditing Commercial Facial Analysis Technology*, in *Medium*, 2019, *https://medium.com/@bu64dcjrytwitb8/on-recent-research-auditing-commercial-facial-analysis-technology-19148bda1832, [https://perma.cc/ W7SJ-38P2*].

[128]Cfr., BUOLAMWINI Joy, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, in *Time*, 2019, *http://time.com/5520558 artificial-intelligence-racial-gender-bias, [https://perma.cc/9USJ-K94C*].

[129]Cfr., GARVIE Clare & FRANKLE Jonathan, *Facial-Recognition Software Might Have a Racial Bias Problem*, in *Atlantic* , 2016, *https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991*, [*https://perma.cc/4L5J -AXR4*].

Nell'ambiente informati così discute molto sui principi di equità[130]. Il primo argomento dibattuto è proprio legato all'incerta definizione di equità ''digitale''. Potrebbe essere definita, ad esempio, come non discriminazione (basata su una particolare caratteristica), o "equità" come ''scelta equa tra gruppi[131]'', o come sinonimo di "correttezza" intesa come preferenza di falsi positivi a falsi negativi[132], o "correttezza" intesa come ''selezione casuale[133]'', o come una miriade di altre definizioni, ognuna delle quali, a seconda del significato attribuitole, può modellare il modo in cui viene sviluppato un modello di apprendimento automatico e i suoi scopi[134].

Nella progettazione di un meccanismo computerizzato intelligente, l'esito del modello può essere influenzato direttamente dal tipo di equità ritenuto corretto o idoneo alle finalità sistemiche[135]. Tuttavia, nel mondo reale, questo *design* di progettazione potrebbe portare a un'applicazione pregiudizievole verso alcuni individui.

Infine, sussistono problemi di trasparenza, relativamente al fatto che le tecnologie alla base della c.d. "scatola nera" sono spesso coperte da segreti commerciali o industriali. Resta, altresì, la difficoltà di attribuzione della responsabilità[136]. In altre parole, dato tutti questi sistemi di riconoscimento del volto e in generale le tecnologie di *machine-learning*, essendo in grado di

---

[130]Cfr., ZHONG Ziyuan, *A Tutorial on Fairness in Machine Learning*, in *Medium*, 2018, *https://towardsdatascience.com/a-tutorial-on-fairness-in-machine-learning-3ff8ba1040cb, [https://perma.cc/HL42-9ZEJ*] .

[131]Cfr., FERGUSON Andrew Guthrie, *Facial Recognition and the Fourth Amendment*, 2019, in *Minnesota Law Review*, 2021, 1105, 105, Available at SSRN: *https://ssrn.com/abstract=3473423* or *http://dx.doi.org/10.2139/ssrn.3473423*, 162.

[132]*Ibidem.*

[133]*Ibidem.*

[134]Cfr., SELBST Andrew D., DANAH BOYD, FRIEDLE Sorelle A. r, VENKATA SUBRAMANIAN Suresh & VERTESI Janet, *Fairness and Abstraction in Sociotechnical Systems*, in *Conf. on fairness, accountability & transparency*, 2019, 59 *https://dl.acm.org/doi/ pdf/10.1145/3287560.3287598, [https://perma.cc/V79B-WULJ*]; BERK Richard, HEIDARI Hoda, JABBARI Shahin, KEARNS Michael & ROTH Aaron, *Fairness in Criminal Justice Risk Assessments: The State of the Art*, in *Socio. Methods & Sch.*, 12 e 15, *https://arxiv.org/pdf/1703.09207.pdf, [https://perma.cc/W86U-9DP7*].

[135]*Ibidem.*

[136]Cfr., JOH Elizabeth E., *The Undue Influence of Surveillance Technology Companies on Policing*, in *N.Y.U L. REV. ONLINE*, 2017, 19-20, 92. *https://www.nyulawreview.org/wp-content/uploads/2017/08/NYULawReviewOnline-92-Joh_0.pdf, [https:// perma.cc/AX4Z-TGGR*]; MITTELSTADT Brent, RUSSELL Chris &WACHTER Sandra, *Explaining Explanations in AI*, CONF. ON FAIRNESS, ACCOUNTABILITY & TRANSPARENCY 2019, 279.

elaborare processi analitici autonomi dagli input umani, non si sa a chi imputare la responsabilità in caso di errori applicativi, risultando difficoltoso determinare dove finisce il linguaggio di programmazione umano e dove inizia il ragionamento autonomo della macchina.

Gli studiosi dell'intelligenza artificiale e dell'apprendimento automatico, pur avendo a lungo tentato di trovare una soluzione che elimini tali problematiche, riscontra, comunque, le medesime questioni di trasparenza, segretezza, responsabilità, imperscrutabilità e interpretabilità[137]. Anche se le macchine diventano sempre più sofisticate e le società di intelligenza artificiale e apprendimento automatico entrano in contatto con della polizia, collaborandovi, resta, ugualmente, la difficoltà di agire in un'ottica di trasparenza, a causa del conflitto tra la necessità delle forze dell'ordine di conoscere il funzionamento dei modelli complessi alla base delle tecnologie facciali e di intelligenza artificiale in generale, e gli interessi contrapposti dei proprietari di questi sistemi, che desiderano mantenere il segreto per vantaggi di mercato[138].

4. Rischi e pericoli cagionati dall'uso del riconoscimento facciale mediante IA su larga scala

Il riconoscimento facciale[139] è una tecnologia che rientra nel campo della biometria[140]che, analizza, attraverso un *software*, le immagini, rappresentanti

[137]Cfr., SELBST Andrew D. & BAROCAS Solon, *The Intuitive Appeal of Explainable Ma- chines*, in *Fordham* , 2018, 1085, 1090, 87 .

[138]Cfr., FERGUSON Andrew Guthrie, *Facial Recognition and the Fourth Amendment*, 2019, in *Minnesota Law Review*, 2021, 1105, 105, Available at SSRN: *https://ssrn.com/abstract=3473423* or *http://dx.doi.org/10.2139/ssrn.3473423*, 169.

[139]Cfr., Nella dottrina giuridica interna, un lavoro monografico dedicato al tema è quello di MOBILIO G., *Tecnologiedi riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, *Editoriale Scientifica*, Napoli, 2021; v. anche, da un'angolazione processual-penalistica, SACCHETTO E., Face to face: il complesso rapporto tra automated facial recognition technology e processo penale, in *www.lalegislazionepenale.it*, 2020. Per una ricognizione della materia da una prospettiva penalistica, con specifico riguardo al contesto statunitense, cfr. *New York City Bar, Power, Pervasiness and Potential: the Brave New World of Facial Recognition Through a Criminal Law Lens (and beyond)*, 2020, in *http://documents.nycbar.org.s3.amazonaws.com/files/2020662-BiometricsWhitePaper.pdf*.

[140]Cfr., l'art. 4, n. 14) del Regolamento Generale sulla Protezione dei dati (GDPR) definisce i dati biometrici come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle

individui, sotto forma di *pixel*, cioè di dati che un modello matematico interpreta e confronta con quelli ricavati da altre immagini. In tal modo, correlando i dati raccolti, si mira a trovare una corrispondenza tra immagini.

Per questa loro peculiarità, le tecniche di riconoscimento facciale possono essere applicate su territori vastissimi ed essere utilizzate nel settore commerciale per aumentare la vendita dei prodotti, e, in quello della pubblica sicurezza, per la prevenzione o repressione del crimine[141]. Ad oggi, tali tecnologie, sempre più avanzate, riescono a riconoscere anche un volto coperto da una mascherina.

L'utilizzo, sempre più diffuso dei *social network*, invece, ha comportato la capacità di identificazione delle persone mediante i metadati o i c.d. *tag*. In altre parole, gli stessi utenti ''taggando''[142] i propri *follower* in una foto condivisa, rivelano alle macchine a chi corrisponde quel volto. L'evoluzione sempre più sofisticata dei *facial recognition systems* è legata anche a precise scelte di *business*, che sollecita le imprese private ad elaborare nuovi, e più precisi, modelli matematici, da vendere alle amministrazioni governative e alle agenzie di controllo o, di supporto in realtà belliche.

Per fare degli esempi, nel marzo del 2022, nel corso dell'invasione Russa in Ucraina, è stata arrestata una attivista russa, identificata grazie al sistema di riconoscimento facciale *Sphere*, installato sui trasporti pubblici di Mosca, qualche giorno dopo aver pubblicato su *Twitter* un commento su una manifestazione contro la guerra tenutasi in piazza *Pushkinskaya*.

Ugualmente, sempre relativamente al conflitto russo-ucraino, la società *Clearview AI*, una *startup* che vende alle imprese e agenzie di controllo pubbliche servizi di riconoscimento facciale basati su algoritmi che utilizzano

caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici». Essi rientrano, dunque, nell'elenco delle particolari categorie di dati di cui all'art. 9 del medesimo Regolamento, il cui trattamento è pertanto sottoposto a un regime di maggior tutela, con la possibilità, espressamente prevista dal medesimo art. 9, per ciascuno Stato di prevedere ulteriori restrizioni a simili trattamenti proprio allorquando si tratti di dati biometrici.

[141]Cfr., CARRER L., *La Russia usa il riconoscimento facciale su chi manifesta contro la guerra*, 2022, in *www.wired.it.*; CARBONI K., *La più controversa startup di riconoscimento facciale sta collaborando con l'Ucraina*, 2022, in *www.wired.it.*

[142]Cfr., ZORLONI L., *Ho scoperto che la più discussa società di riconoscimento facciale al mondo ha le mie foto*, 2021, in *www.wired.it.*

i metadati, raccolti dai *social network* senza consenso delle persone interessate, si è offerta di aiutare il governo ucraino mettendo a disposizione i propri servizi per individuare infiltrati russi, riunire i rifugiati con le proprie famiglie e a identificare le persone morte durante la guerra. Questo metodo di raccolta dativolto a consentire la‘’profilazione’’[143]e la sorveglianza delle persone, ha condotto alcuni Stati, tra cui l'Italia[144] a ritenere l'attività di *Clearview AI* contraria alla legge.

In effetti, se da un lato, l'utilizzo delle tecniche di riconoscimento facciale, si sono rivelate molto utili, dall'altro, molte critiche vengono mosse in relazione al fatto che con il loro utilizzo, si violi reiteratamente il diritto di *privacy*, trattando i dati personali in maniera scorretta, e adottando forme di sorveglianza di massa[145]. Questi sistemi, quindi, spesso ledono e limitano, profondamente, i diritti fondamentali e costituzionalmente garantiti della personalità, nonché di riunione, associazione e libera manifestazione del pensiero[146].Le TRF provocano, in buona sostanza, il *c.d.chilling effect*[147]cioè una forma di auto-censura da parte della popolazione che, sentendosi controllata dai sistemi di videosorveglianza, limita l'esercizio dei suoi diritti fondamentali.

I rischi causati dall'uso improprio e distorto di queste tecnologie, (basti pensare alla Cina dove il riconoscimento facciale è stato definito un genocidio

[143]Cfr., Ai sensi dell'art. 4 del GPDR, per profilazione s'intende «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica,la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

[144] Il Garante privacy sanziona *Clearview AI* per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio.

[145]Da intendersi come la «raccolta ed elaborazione di dati personali, identificabili o meno, allo scopo di influenzare o controllare coloro ai quali essi appartengono»: così, LYON D., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, in FELTRINELLI (a cura di), Milano, 2002, 2. V. anche ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, in RAFFAELLO CORTINA EDITORE (a cura di), Milano, 2015.

[146]Cfr., G MOBILIO., *Tecnologie di riconoscimento facciale, cit.*, 57 ss.

[147]Cfr.,Sul c.d. *chillingeffect*, tra i contributi più recenti, v. VIGANÒ F., *La proporzionalità della pena. Profili di dirittopenale e costituzionale*, Torino, 2021, 277 ss.; RECCHIA N., *Il principio di proporzionalità nel diritto penale*, Torino, 2020, 252 ss.

culturale della popolazione Uiguri[148]) ha indotto molti Paesi a vietarne o, limitarne l'uso.

In Italia, evidenziati i rischi delle TRF, non è mai stato autorizzato il riconoscimento facciale in modalità "*real time*"[149], ritenuta illegittima dal Garante per la protezione dei dati personali poiché carente di una regolamentazione *ad hoc* e perché ritenuto lesivo dei diritti fondamentali della persona, a causa delle vere e proprie forme di sorveglianza di massa nei luoghi pubblici e della notevole interferenza della sfera personale del cittadino, spesso ignaro di essere controllato. Per questo, con decreto-legge n. 51 giugno 2023, l'Italia ha confermato il divieto di installare sistemi di riconoscimento facciale nei luoghi pubblici, nei negozi o sui cartelloni pubblicitari, fino a dicembre 2025, senza eccezione alcuna, "salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero".

Anche il governo americano, che notoriamente fa largo uso del TRF, ne ha limitato l'applicazione da parte della polizia, e ha sospeso l'utilizzo del software *Rekognition* di proprietà di Amazon e l'uso di altri elaborati da *Microsoft* e IBM, per ridefinirne i contorni normativi e per evitare lesioni di diritti fondamentali.

La tecnologia di riconoscimento facciale sviluppata da Amazon, dal nome *Rekognition*, operante sul mercato dal 2016, è stata descritta come «servizio che semplifica l'aggiunta di analisi delle immagini alle applicazioni e rileva oggetti, scene e volti nelle immagini». Il software è risultato fortemente discriminatorio nei confronti delle persone di colore[150] e gli errori identificativi derivano dal fatto che la percentuale di immagini di volti di colore, nella programmazione del sistema, è minore rispetto alle immagini rappresentanti volti bianchi, per cui l'algoritmo è maggiormente allenato a trovare questi

[148]V.,ad es., CLARKE M., *Framing the Xinjiang emergency: colonialism and settler colonialism as pathways to cultural genocide?*, in ID. (a cura di), *The Xinjiang emergency Exploring the causes and consequences of China's mass detention of Uyghurs*, 10 ss. Più ampiamente, infra par. 4.

[149]Cfr., GARANTE PER LA PROTEZIONEDEI DATI PERSONALI, Parere sul sistema SARIreal time, 25 marzo 2021.

[150]È il risultato di uno studio dal titolo "*Gender Shades*" condotto da BUOLAMWINI Joy, ricercatrice del *M.I.T. Media Lab.*

ultimi. Questo sistema, avente un processo di apprendimento automatico, consente un confronto istantaneo tra le foto contenute nei *database* di sistema e le immagini prelevate da un account *online* di un *social media*. Il punto problematico è che questo software è stato utilizzato alle forze di polizia in totale segretezza, ledendo la sfera personale degli individui, per identificare i partecipanti a manifestazioni pubbliche potenzialmente pericolosi.

Per tali motivi, nel 2020, Amazon ha sollecitato il Congresso a promulgare norme più rigorose, al fine di evitare l'uso distorto delle tecniche di riconoscimento facciale e, in attesa di ciò, ha sospeso il servizio di *Rekognition* alle autorità di polizia statunitensi per dodici mesi.

Due anni prima, nel 2018 anche il colosso Microsoft, proprio per far fronte al difficile equilibrio tra "*social responsibility"* e *"market success*", in assenza di una chiara regolamentazione normativa, ha posto a base dell'utilizzo dl riconoscimento facciale, i seguenti principi i c.d. *Facial Recognition Principles*: (i) correttezza, per scongiurare trattamenti non equi tra gli interessati; (ii) trasparenza, così da mettere subito al corrente l'utente delle capacità, ma soprattutto dei limiti, delle tecnologie oggi utilizzate per il riconoscimento facciale; (iii) responsabilizzazione, per assicurare un uso delle tecnologie che possa essere sempre controllato dagli utenti; (iv) non discriminazione, per evitare che il riconoscimento facciale possa essere utilizzato per fini o con risultati discriminatori;(v) informazione e consenso, così da assicurare che la tecnologia sia utilizzata sempre previo consenso dell'interessato; (vi) divieto di utilizzo improprio delle tecnologie di riconoscimento facciale per scopi di sorveglianza di massa[151].

[151]Cfr., COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema Penale—SP*, , 9, 2022, 24 e 27.

Gradualmente anche in America si è acquisita la consapevolezza che l'utilizzo degli strumenti di riconoscimento facciale da parte delle autorità di polizia dovesse essere regolato con specifici e dettagliati provvedimenti normativi per evitare pericolose disfunzioni.

La prima città a dare un segnale in tal senso è stata San Francisco che con un'ordinanza del 21 maggio 2019, ha vietato alla autorità di polizia in maniera definitiva, di utilizzare gli strumenti di riconoscimento facciale nelle aree pubbliche.[152]. La decisione è stata giustificata dalle evidenti criticità legate all'uso di tali sistemi rispetto alla tutela dei diritti fondamentali e alla luce del rischio di abusi.

Successivamente, l'iniziativa di San Francisco è stata adottata anche da molte altre città americane[153].

5. Analisi comparatistica dei quadri normativi di Stati Uniti, Ue, Regno Unito

Dopo aver chiarito cos'è il riconoscimento facciale in generale e come funziona, è necessario volgere lo sguardo alle discipline legislative dei singoli Stati; in particolare negli Stati Uniti, nell'Ue, e nel Regno Unito.

Preliminarmente occorre ribadire che, negli ultimi tempi, la discussione concernente l'impiego nella giustizia penale dei nuovi dispositivi tecnologici[154], basati su sistemi di IA, è al centro del dibattito giurisprudenziale

[152]Cfr.,La notizia ha avuto un significativo clamore mediatico. Si veda, ad esempio, LEED., *San Francisco is first US city to ban facial recognition,* in *BBC News,* 2019 *;* CONGER K., FAUSSET R. and KOVALESKI S. F., *San Francisco Bans Facial Recognition Technology,* in *The New York Times,* 2019*; V.* DUBAL, *San Francisco was right to ban facial recognition. Surveillanceis a realdanger,* in *The Guardian,* 2019.

[153] Si segnala lo stop nelle città di Oakland, 2019; Boston 2020 e Portland (ordinanza del 4 novembre 2020).

[154]Cfr., DELLA TORRE Jacopo, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice,* in *Diritto Penale Contemporaneo—DPC,* fascicolo n. 1, 2020, 232.

e dottrinale[155] dei Paesi extraeuropei[156]ed europei[157](tra cui, chiaramente rientra anche l'Italia).

Infatti, seppur è evidente il grande aiuto investigativo, di prevenzione e di repressione del crimine, derivante dall'uso della polizia di queste nuove tecnologie, rimangono innumerevoli criticità[158] quali scarsa affidabilità, correlata alla scarsa qualità delle immagini, alla luce e altri fattori[159] ed effetti

[155] Tra gli autori più noti sono da citare: BARBARO, 2018, COSTANZI, 2018; PAGALLO e QUATTROCOLO, 2018; ZAVRŠNIK, 2018; BASILE, 2019; CONTISSA *et. al*, 2019; D'AGOSTINO, 2019; EAD., 2018—2019; GIALUZ, 2019; MALDONATO, 2019; NIEVA-FENOLL, 2019; OCCHIUZZI, 2019; PARODI e SELLAROLI, 2019; QUATTROCOLO, 2019.; RICCIO , 2019 ; TRAVERSI , 2019; ZIROLDI, 2019.

[156] V., Ci si riferisce, ad esempio, alla Cina (LI e CADELL, *China eyes "black tech" to boost security as parliament meets*, in *www.reuters.com*, 2018; MOZUR e KROLIK, *A Surveillance Net Blankets China's Cities, Giving Police Vast Powers*, in *www.nytimes.com*, 2019), all'India (v. TOUSSAINT, *Indian police are using facial recognition to identify protesters in Delhi*, in *www.fastcompany.com*, 2019; Zaugg, *India is trying to build the world's biggest facial recognition system*, in *edition.cnn.com*, 2019, alla Russia (VINCENT, *Moscow rolls out live facial recognition system with an app to alert police*, in *www.theverge.com*, 2020) e agli StatiUniti (BRANDOM, *Police are using facial recognition the wrong way. And altering our faces?*, in *www.theverge.com*, 2019; COLLINS, *Facial recognition: Do you really control how your face is being used?*, in *eu.usatoday.com*, 2019; HAMANN e SMITH, *Facial Recognition Technology: Where Will It Take Us?*, in *www. americanbar.org*; GARVIE, BEDOJA, FRANKLE, *The perpetual line-up. Unregulated police face recognition in America*, in *https://www.perpetuallineup. org/*, 2016; GARVIE e MOY, *America under Watch. Face surveillance in the United States*, in *https://www.americaunderwatch.com/*, 2019; Shuppe, *How facial recognition became a routine policing tool in America*, in *www.nbcnews.com*, 2019; VALENTINO- DEVRIES, *How the Police Use Facial Recognition, and Where It Falls Short*, in *www.nytimes.com*, 2020). È bene, peraltro, precisare che la tecnologia in esame è anche utilizzata dall'INTERPOL: in: *https://www.interpol.int/How-we-work/Forensics/Facial-Recognition.*

[157]Cfr., *report* dell'EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 11 ss. Una più ampia mappatura delle autorità di *law enforcement UE* che adoperano i meccanismi in questione è reperibile, consultando il seguente articolo: KAYSER-BRIL, *At least 10 policeforces use face recognition in the EU, AlgorithmWatchreveals,*; in *https://algorithmwatch.org/en/story/face-recognition-police-europe/*.

[158] V. CARLO S., *Face off. The lawless growth of facial recognition in UK policing*, in *Big Brother Watch*, 2018; cfr., COUCHMAN Hannah, *Artificial Intelligence: what it is and why you should care*, in *Liberty*, 2017, *www.libertyhumanrights.org.uk*,; cfr., GOV.UK , *Facial Recognition Working Group of the Biometrics and Forensics Ethics Group, Ethical issues arising from the police use of live facial recognition technology*, 2019 ; cfr., FUSSEY e MURRAY, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, in HUMAN RIGHTS CENTRE, UNIVERSITY OF ESSEX, (diretto da); cfr., *Final report on live facial recognition*, in *London Policing Ethics Panel*, 2019, 42 ss.; cfr., LYNCH J., *Face Off Law enforcement use of face recognition technology* in *Social Science Research Network*, 2020; cfr, studio di GARVIE e MOY, *America under watch*, 2016, in https://www.americaunderwatch.com/

[159] V., il recente studio di GARVIE, *Garbage in, Garbage Out. Face Recognition on Flawed Data*, al presente link: *https://www.flawedfacedata.com.*

discriminatori[160], confermate da innumerevoli studi[161]. Sul punto si è pronunciato il *National Institute of Standards and Technology*[162]degli Stati Uniti che ha condotto numerosi esperimenti sugli algoritmi di *facial recognition* in commercio, concludendo che la maggior parte di questi sistemi commette innumerevoli errori (*bias*), o imprecisioni, specie se si tratta di identificare donne afroamericane e asiatiche, meno difficoltà sono state riscontrate, invece, nel caso di identificare i caucasici[163].

Un altro aspetto altamente problematico è quello relativo alla lesione della privacy legata all'uso di questi meccanismi di sorveglianza di massa, soprattutto se applicati su larga scala[164]. Dopo il c.d. ''scandalo di *Clearview*'', avvenuto negli Stati Uniti, tuttavia, e a seguito di un'inchiesta del *New York*

---

[160]Cfr., GARVIE e FRANKLE, *Facial-Recognition Software Might Have a Racial Bias Problem*, in *www.theatlantic.com*, 2016; EAD., *When the Robot Doesn't See Dark Skin*, in *www.nytimes.com*, 2018; LOHR, *Facial Recognition Is Accurate, if You're a White Guy*, in *www.nytimes.com*, 2018; BUOLAMWINI, *Response; Racial and Gender bias in Amazon Rekognition – Commercial AI System for Analyzing Faces*, in *www.medium.com*, 2019; BUOLAMWINI e GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*; *Concerned Researchers, On Recent Research Auditing Commercial Facial Analysis Technology*, in *www.medium.com*, 2019; HARMON, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias*, in *www.nytimes.com*, 2019; HOGGINS, *'Racist and sexist' facial recognition cameras could lead to false arrests*, in *www.telegraph.co.uk*; MORRISON, *"Racist" facial recognition technology used in law enforcement, banking and schools misidentifies African American and Asian people 100 times more often than whites, study shows*, in *www.dailymail.co.uk*, 2019. PORTER, *Federal study of top facial recognition algorithms finds "empirical evidence" of bias*, in *www.theverge.com*, 2019; Pare utile ricordare che, preso atto di tale criticità, l'*EUROPEAN DATA PROTECTION BOARD*, nelle sue *Guidelines 3/2019 on processing of personal data through video devices*, adottate il 10 luglio 2019, ha affermato che «*bias in facial recognition threatens to reinforce the prejudices of society. That is why, data controllers must also ensure that biometric data processing deriving from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided*».

[161]Cfr.,DELLA TORRE Jacopo, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Dirtto Penale Contemporaneo—DPC*, fascicolo n. 1, 2020, 232 e 236.

[162] V., il recente studio di GROTHER, NGAN, HANAOKA, *Face Recognition Vendor Test (FVRT). Part 3: Demographic Effects*, consultabile al presente link: *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf*, p. 2 e ss; v. anche *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, in *www.nist.gov*, 2019, nonché SINGER e METZ, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, in *www.nytimes.com*, 2019.

[163]Cfr., DELLA TORRE Jacopo, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Dirtto Penale Contemporaneo—DPC*, fascicolo n. 1, 2020, 232 e 236.

[164]Cfr., CHANDRAN, *Mass surveillance fears as India readies facial recognition system*, in *www.reuters.com*, 2019; GARVIE e MOY, *America under watch*, (cit. ''Lo scorso anno ha fatto, ad esempio, assai scalpore l'utilizzo da parte della polizia cinese della tecnologia in esame per individuare e controllare la minoranza musulmana degli Uiguri''); cfr. MOZUR, *OneMonth, 500.000 Face Scans: How China Is Using A.I. to Profile a Minority*, in *www.nytimes.com*, 2019.

Times[165], c'è stata una spinta legislativa volta a disciplinare, a livello normativo, in modo più dettagliato, i presupposti e i limiti legati all'uso di questi software avanzati[166]. In alcune città, addirittura, come San Francisco, Somerville, Oakland e in Stati come la California[167] è stato posto il divieto, per le forze di polizia, di continuare ad utilizzare questi strumenti tecnologici avanzati o, in altri Stati limitatamente una categoria maggiormente invasiva di questi.

Anche in UE, dove lo scetticismo legato all'uso dei sistemi di riconoscimento facciale è ampiamente più elevato rispetto agli Stati Uniti, l'Agenzia dell'Unione Europea per i diritti fondamentali, ha dichiarato che il tema in esame rientra in assoluti da quelli meno trattati dalla disciplina legislativa e dalle Corti[168].

Sul punto, la *High Court of Justice* dell'Inghilterra e del Galles si è pronunciata nel 2019[169], analizzando in concreto per la prima volta la compatibilità dell'utilizzo da parte della polizia di mezzi di riconoscimento facciale con i diritti fondamentali alla riservatezza e alla tutela dei dati personali. Da questa prima svolta legislativa anche molti altri stati hanno disciplinato in modo più preciso e rigoroso la disciplina ''facciale''.

Fatta questa premessa, è possibile passare all'analisi del quadro applicativo dei *software* di *face recognition* nei singoli Stati.

Negli Stati Uniti, a causa delle frequenti problematiche legate agli errori dei sistemi di rilevamento del volto, si è tentato di porre rimedio agli usi distorti

---

[165]Cfr., HILL, *The Secretive Company That Might End Privacy as We Know It*, in *www.nytimes.com*, 2020; HILL, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, in *www.nytimes.com*, 2020, oppure il Procuratore generale del New Jersey a vietare alla polizia di avvalersi tale *software;* HILL, *New Jersey Bars Police From Using Clearview Facial Recognition App*, in *www.nytimes.com*, 2020.

[166] V., SCHNEIER, *We're Banning Facial Recognition. We're Missing the Point*, in *www. nytimes.com*, 2020; cfr. TECH POLICY, *40 groups have called for a US moratorium on facial recognition technology*, in *Mit Technology Review*, 2020.

[167]V. *California Governor Signs Landmark Bill Halting Facial Recognition on Police Body Cams*, in *www.aclunc.org*; nonché METZ, *California lawmakers ban facial-recognition software from police body cams*, in *www.edition.cnn.com*, 2019.

[168]V. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *Facial recognition technology*, cit., 4, ove si afferma che, in questa materia, «*case law is still virtually non-existent*».

[169]Cfr., LIBERTY, *Liberty fights for facial recognition ban following Court ruling*, nonché DEARDEN, *Police used facial recognition technology lawfully, High Court rules in landmark challenge*, in *www.independent.co.uk*, 2019.

delle TRF per evitare che la polizia, che faccia uso di tecnologie di sorveglianza, identificazione, tracciamento e verifica facciale[170],incorra in errori di valutazione. Non è però allo stato prevista una specifica disciplina normativa.

Passando al panorama europeo, nell'ottica della prevenzione dei rischi connessi alla violazione dei diritti fondamentali, derivanti dall'utilizzo delle TRF, in Europa il Parlamento Europeo, già dal 2019, con la Risoluzione su "Una politica industriale europea globale in materia di robotica e intelligenza artificiale"[171] aveva manifestato dubbi e preoccupazioni sull'impiego dell'intelligenza artificiale, in particolare, sulle tecniche di riconoscimento facciale e vocale, e sui programmi di "sorveglianza emotiva", utilizzati per monitorare lo stato d'animo dei lavoratori e dei cittadini.[172]

Successivamente, nel 2020, con il *White paper*, la Commissione Europea aveva sollevato dubbi in merito alla identificazione biometrica a distanza perché lesiva dei diritti fondamentali[173].

Ancora, in seguito, anche il Garante Europeo per la protezione dei dati[174] e il Parlamento Europeo[175] hanno adottato lo stesso orientamento. La Commissione Europea, il 21 aprile 2021, ha pubblicato l'*Artificial Intelligence Act* (che si inserisce nel contesto della c.d. strategia *"a Europe fit for the digital age", ossia* un'Europa adatta all'era digitale[176]), una proposta di regolamento

---

[170]Cfr., FERGUSON Andrew Guthrie, *Facial Recognition and the Fourth Amendment*, 2019. 105 in *Minnesota Law Review*, 2021, 1105,105 Available at SSRN: *https://ssrn.com/abstract=3473423* or *http://dx.doi.org/10.2139/ssrn.3473423*, 193.

[171]V., *https://www.altalex.com/documents/news/2023/06/23/ai-act-ue-traccia-futuro-intelligenza-artificiale.*

[172]Cfr. PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale, 2088,* 13, *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52019IP0081*.

[173]Cfr. EUROPEAN COMMISSION, *White Paper on Artificial Intelligence: a European approach to excellence and trust*, 2020, 20 ss., *https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_it.*

[174]Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust*,2020 66, *https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf.*

[175]Cfr. EUROPEAN PARLIAMENT, RESOLUTION *"Artificial intelligence: questions of interpretation and application of international law"*, 2021, 0009, 56, *https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html.*

[176] V., *https://www.altalex.com/documents/news/2023/06/23/ai-act-ue-traccia-futuro-intelligenza-artificiale.*

volta al controllo e alla valutazione dei rischi in relazione all'uso delle tecniche di IA[177].

Il 6 ottobre 2021, con la Risoluzione ‘*’Artificial Intelligence in Criminal Law and its use by the police judicial authorities in criminal matters’’*, il Parlamento Europeo, esaminando il tema dei rischi di grave lesività dei diritti degli individui legati all'uso di una sorveglianza facciale di massa, ne ha vietato l'uso. In particolare, si è evidenziata la grave violazione dei principi della presunzione di innocenza o del giusto processo qualora il sistema penale dovesse diventare di tipo ‘’preventivo’’; in altre parole, se la polizia potesse avere accesso a questi sistemi di riconoscimento esclusivamente per verificare la potenziale colpevolezza o meno di un determinato individuo, ledendo così la sua sfera privata personale, i più importanti principi che fondano il sistema penale verrebbero irrimediabilmente violati, eliminando le garanzie processuali dei cittadini. In definitiva, l'utilizzo di dati biometrici, a fini identificativi, a causa della loro stretta connessione con il principio di dignità umana, meritano una protezione rafforzata, che non potrebbe essere assicurata mediante un meccanismo di tracciamento indiscriminato.

Nel giugno 2023, è stato approvato un nuovo testo (in riferimento all' l'*Artificial Intelligence Act* del 2021) da parte del Parlamento Europeo, che dovrà essere oggetto di negoziazione in seno al Consiglio, per poi entrare in vigore non prima del 2025. In virtù di tanto, si è pensato di introdurre un codice di condotta volontario che dovrà essere adottato dalle principali aziende che si occupano di software di IA, nel periodo di "*vacatio legis*".

Nel dettaglio, l'*AI ACT* è una proposta di legge europea sull'intelligenza artificiale che, individua i livelli di rischio collegati alle TRF che si ripercuotono sulla vita delle persone, limitandone fortemente i diritti fondamentali, unitamente alla salute ed alla sicurezza.

L'*AI ACT* distingue i sistemi di intelligenza artificiale in diverse classi di rischio: (i) rischio inaccettabile[178], che sono vietati perché costituiscono una

[177]Cfr. il considerando n. 18, COM, 2021, 206, *https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206*.

[178]Cfr., *https://www.altalex.com/documents/news/2023/06/23/ai-act-ue-traccia-futuro-intelligenza-artificiale.*

minaccia per le persone, come, ad esempio, le tecniche manipolative o ingannevoli per condizionare il comportamento, o le tecniche che sfruttano la vulnerabilità di alcuni individui o gruppi; le TRF in tempo reale e a distanza; tecniche che individuano le emozioni, il divieto di *social scoring* (sistema di credito sociale: il punteggio sociale da parte delle agenzie pubbliche, o la pratica di utilizzare i dati sul comportamento sociale delle persone per fare generalizzazioni e profili) e, così via; (ii) alto rischio[179] che sono quelli che limitano i diritti fondamentali, sulla sicurezza e sulla salute, nel cui ambito rientrano anche i rischi ambientali derivanti da infrastrutture o reti di gestione energetica o idrica, i trasporti, gestione della migrazione ecc. (iii) Vi sono, poi, il rischio limitato[180] ed il rischio minimo[181]. Il primo è riferibile ai sistemi di IA con specifici obblighi di trasparenza; il secondo si riferisce ai sistemi che possono essere liberamente utilizzati, come ad esempio, applicazioni su videogiochi abilitati alla intelligenza artificiale o filtri antispam.

Naturalmente, più è alto il rischio più la regolamentazione normativa sarà restrittiva.

In sintesi, l'obiettivo del programma europeo è quello di regolamentare l'utilizzo dei sistemi di intelligenza artificiale, in modo tale che sia garantita la sicurezza, la trasparenza, la tracciabilità, l'assenza di discriminazione, il rispetto dell'ambiente.

Nell'*AI ACT*, relativamente al divieto di utilizzo delle tecniche di IA, sono state introdotte tre macro-eccezioni[182]nei casi in cui esse siano di ausilio alle forze dell'ordine, in contesti caotici e di grandi assembramenti, per mantenere la pubblica sicurezza. Il loro impiego sarebbe consentito per: trovare potenziali vittime di reato, compresi minori scomparsi; impedire minacce specifiche, sostanziali ed imminenti alla vita ed all'incolumità personale (es attacco terroristico)[183]; individuare, localizzare, identificare o perseguire soggetti

[179]*Ibidem.*

[180]*Ibidem.*

[181]*Ibidem.*

[182]Cfr. l'art. 5 par. 1, lett. *d*), 2021/0106(COD).

[183]Cfr., *https://www.agendadigitale.eu/sicurezza/privacy/riconoscimento-facciale-lapproccio-italiano-e-in-antitesi-alla-ue-i-nodi/.*

sospettati di reato di cui all'art. 2 paragrafo 2 della decisione quadro 2002/584/GAI del Consiglio[184], punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà, della durata massima di almeno tre anni, come stabilito dalla legge di tale stato membro[185].Naturalmente tale utilizzo subirà limitazioni temporale, geografiche e personali e sarà proporzionato alla gravità ed alla probabilità che un danno o un evento possa verificarsi, valutando anche la gravità delle relative conseguenze.

Tale apertura a ragioni di pubblica sicurezza lascia lo spazio a vari dubbi interpretativi[186], sull'utilizzo dei sistemi di IA, dal momento che la loro adozione sarebbe in ogni caso sottoposta ad una autorizzazione giudiziaria o amministrativa regolata da diverse leggi nazionali anche relativamente alla pena edittale, che varia da stato a stato.

Nel Regno Unito, infine, molti corpi di polizia stanno sperimentando, negli ultimi anni, la tecnologia del *facial recognition*, ai fini di prevenzione e repressione della criminalità, attraverso una serie di progetti pilota[187] avviati, tuttavia, in assenza di una disciplina legislativa *ad hoc* che regoli la fattispecie in esame[188].

Tra tutti i dipartimenti la *South Wales Police*[189] ha assunto un ruolo preminente nell'uso di queste *new tecnologies,* avviando, grazie ad ingenti finanziamenti governativi, un progetto di analisi relativo all'efficacia del riconoscimento facciale[190]. Il programma studia l'utilizzo dei *software* facciali,

[184]*Ibidem.*

[185]Cfr. l'art. 61, 2021/0106(COD).

[186]Cfr. l'art. 3 par. 35, 2021/0106(COD).

[187] Riferimento alla *London Metropolitan Police*, alla *South Wales Police* e alla *Leicestershire Police*: in proposito, v. THE LAW SOCIETY OF ENGLAND AND WALES, *Algorithms in the Criminal Justice System*, 2019, 37 s., nonce l'ampio studio di PURSHOUSE E CAMPBELL, 2019,188 ss.

[188]Cfr., BIG BROTHER WATCH, *Face off*, cit., 9; PURSHOUSE e CAMPBELL, 2019, 198; FUSSEY e MURRAY D., *Independent Report on the London Metropolitan Police Service's*, cit., 49; THE LAW SOCIETY OF ENGLAND AND WALES, *Algorithms in the Criminal Justice System*, cit., 41.

[189]ID., PURSHOUSE e CAMPBELL, 2019, 190.

[190]V., South Wales Police website: *http://www.afr.south-wales.police.uk.*

tramite due metodologie: (i) "l'*AFR Identify*"[191] che studia l'analisi statistica di successo del meccanismo di *matching* tra un soggetto ignoto, rilevato dalla telecamere, e i cinquecentomila profili facciali presenti nei *database* della polizia di *South Wales*[192], tramite un apposito algoritmo di *facial recognition*; (ii) *"*l'*AFR Locate"* che è un sistema di ripresa *live*, in *real-time* che usufruisce di telecamere posizionate nelle città, il cui scopo è meramente quello di controllo generalizzato e di acquisizione di quante più informazioni facciali possibili, per registrarle negli archivi[193] e per confrontarle, in un secondo momento, mediante appositi *software*, con i modelli biometrici di individui inseriti in una lista *ad hoc*, più ristretta, la c.d.*''watch list''* (spesso contenente informazioni di soggetti potenzialmente pericolosi), elaborata a seconda del singolo caso investigativo dalla *South Wales Police*[194].

Se i software riscontrano una corrispondenza tra due profili biometrici, allora le due immagini vengono ricontrollate da un c.d. *''AFR operator'',* anche detto *''the system operator''*; si tratta di un agente di polizia che ha il compito confermare il *match*, onde evitare errori di sistema[195]. Il fatto che un operatore ''umano'' debba sempre intervenire, soprattutto nella fase finale dell'attività del *tool*, rappresenta una grande garanzia, tale da ridurre seppur non eliminare totalmente[196]la probabilità che un soggetto sia ingiustamente arrestato a causa di valutazioni algoritmiche imprecise[197].

Da un punto di vista pratico, il *facial recognition*, in particolare *l'AFR Locate*, nel Regno unito, è stato utilizzato, ad esempio, dalla polizia gallese in più di cinquanta occasioni tra maggio 2017 e l'aprile 2019 durante i pubblici

[191]Cfr., DELLA TORRE Jacopo, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Dirtto Penale Contemporaneo—DPC*, fascicolo n. 1, 2020, 232 e 236.

[192]Cfr. [2019] EWHC 2341 § 27, R (Bridges) v *Chief Constable of South Wales Police, (Administrative Court).*

[193]Ivi §§ 28 SS.

[194]Ivi § 31.

[195]Ivi § 33.

[196]V. a tal proposito, l'autorevole dottrina, LOPEZ, *La rappresentazione facciale tramite software*, SCALFATI A., *Le indagini atipiche*, in GIAPPICHELLI (a cura di), Torino, 2019, 244.

[197]Cfr. [2019] EWHC 2341, § 33, *«the fact that human eye is used to ensure that an intervention is justified, is an important safeguard»*

eventi[198]; si ricorda la finale di UEFA *Champions League* di Cardiff del 2017, evento definibile come ''storico'', poiché in quell'occasione è stato compiuto il primo arresto in diretta tramite mezzi di riconoscimento facciale[199].

Gli algoritmi *AFR identify* e *Locator*, tuttavia, sebbene si siano manifestati utili in svariate occasioni, non mancano tassi di errore particolarmente elevati[200], basti pensare che, nella medesima finale di *Champions League* del 2017, prima di ottenere il riscontro corretto, oltre duemila persone sono state erroneamente identificate quali possibili criminali[201] dai *tools*[202].

Sul punto l'Università di Cardiff ha effettuato una ricerca sull'efficacia di questi sistemi da parte della polizia[203], chiarendo che, mediante un miglioramento dell'accuratezza della tecnologia di apprendimento automatico, diminuendo i c.d ''*bias* cognitivi'', le azioni delle forze dell'ordine potrebbero migliorare significativamente[204]. La questione è ancora in evoluzione.

6. Il riconoscimento facciale in Italia

Con il decreto-legge n. 51/2023, l'Italia ha confermato il divieto di installare sistemi di riconoscimento facciale nei luoghi pubblici, nei negozi o sui cartelloni pubblicitari, fino al mese di dicembre del 2025. Ciò senza eccezione alcuna, "salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria

[198]Ivi § 28.

[199]V., per approfondimento BRIDGE, *Police make first arrest using facial recognition surveillance cameras at Cardiff Millennium stadium,* in *www.thetimes.co.uk*, 2017.

[200]Cfr., PURSHOUSE J, CAMPBELL L, *Automated facial recognition and policing: A Bridge too far?, in Legal Studies*, 2022, 209; Id., nota 15 , 191.

[201]Cfr., DELLA TORRE Jacopo, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice,* in *Diritto Penale Contemporaneo—DPC,* fascicolo n. 1, 2020, 236.

[202]V., il seguente articolo della BBC: *2,000 wrongly matched with possible criminals at Champions League*, in *www.bbc.com,* 2018.

[203]V., *report* di DAVIES, INNES, DAWSON, *An Evaluation of South Wales Police's Use of Automated Facial Recognition,* in *https://static1.squarespace.com/static/51b06364e4b02de2f57fd72e/t/5bfd4fbc21c67c2cdd692fa8/1543327693640/AFR+Report+%5BDigital%5D.pdf*.

[204]La citazione è tratta dal seguente ''post'': *Evaluating the Use of Automated Facial Recognition Technology in Major Policing Operations*, reperibile al seguente link: *https://www.cardiff.ac.uk/news/view/1383278-evaluating-the-use-of-automated-facial-recognition-technology-in-major-policing-operations.*

nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero"[205].Con tale decisione l'Italia si è allineata all'orientamento UE.

I privati, quindi, non potranno più installare sistemi di riconoscimento facciale nelle proprie attività commerciali, mentre i Comuni potranno farlo previa autorizzazione del Garante della privacy che però, fino ad ora, ha sempre respinto ogni istanza. L'utilizzo dei sistemi di riconoscimento facciale, per cui, è consentito, senza alcuna moratoria, esclusivamente alla Autorità giudiziaria nell'esercizio delle funzioni giurisdizionali ed al Pubblico Ministero nell'esercizio delle proprie funzioni.[206]

L'Italia, quindi, allineandosi alla posizione Europea, in considerazione del fatto che i sistemi di rilevamento facciale violano i diritti fondamentali, la privacy e risultano profondamente discriminatori, ha sospeso il loro utilizzo, in attesa di una normativa europea *ad hoc*, che colmi le lacune attuali e regoli in maniera chiara le modalità di raccolta ed utilizzo dei dati. Tale necessità è stata evidenziata sia dal garante della privacy nel GDPR, che dalla Direttiva EU 2016/680. In Italia, manca una base normativa in tal senso e le disposizioni richiamate dal Garante della privacy non possono colmare una tale lacuna normativa[207].

Per garantire la tutela dei diritti fondamentali la legge dovrebbe non solo limitarsi ad autorizzare l'utilizzo dei sistemi biometrici, ma dovrebbe anche e

---

[205]V. d.l.51/2023, art 9, *https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.versione=1&art.idGruppo=4&art.flagTipoArticolo=0&art.codiceRedazionale=21A07259&art.idArticolo=9&art.idSottoArticolo=1&art.idSottoArticolo1=10&art.dataPubblicazioneGazzetta=2021-12-07&art.progressivo=0.*

[206]Cfr., *https://www.ilpost.it/2023/06/22/moratoria-riconoscimento-facciale-2025/ https://www.cybersecurity360.it/legal/blocco-del-riconoscimento-facciale-in-italia-proroga-fino-al-2025-per-restare-in-europa/ https://www.wired.it/article/riconoscimento-facciale-sorveglianza-proroga-moratoria-2025-senato/.*

[207]Cfr., Il Garante per la Privacy nel parere del 26 luglio 2018 su SARI ha richiamato l'art. 4 TULPS e l'art. 349 c.p.p. L'art. 4 TULPS e l'art. 349 c.p.p. sono norme che consentono, a determinate condizioni, l'identificazione dei soggetti tramite rilievi segnaletici, purché si tratti di «persone pericolose o sospette» (art. 4 TULPS) o di «soggetti nei cui confronti siano svolte le indagini» (art. 349 c.p.p.). È evidente, dunque, che tali riferimenti normativi non possano rappresentare una base legislativa generale per qualsiasi trattamento.

soprattutto, adottare appositi sistemi di controllo, come regolamenti e norme di condotta, per tutelare i diritti fondamentali, per evitare il rischio di abusi.

Oltre ciò sarebbe opportuno, in una nuova previsione normativa, ridurre l'applicazione di tali tecniche solo ai reati più gravi, dato che un utilizzo generalizzato, può divenire potenzialmente incontrollato, trasformandosi in una sorveglianza di massa.

Relativamente all'aspetto processuale, si evidenzia che attualmente la prova acquisita con i sistemi di riconoscimento facciale, non è valutabile come prova nel processo; questo perché tali strumenti di IA non offrono alcuna validità scientifica. Si auspica, tuttavia, che nel prossimo futuro questi strumenti saranno maggiormente affidabili, al punto da entrare a far parte dei processi in tal senso[208].

7. La posizione del Garante: il SARI ENTERPRICE e il SARI REAL TIME

Con la Risoluzione del Parlamento europeo del 6 ottobre 2021 relativa all'uso della IA nel diritto penale, si è chiesto alla Commissione «una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto con funzione di identificazione»[209], data l'assenza di una regolamentazione specifica volta ad evitare lesioni dei diritti fondamentali e pregiudizi discriminatori a carico dei cittadini e anche per porre l'attenzione sul preoccupante «utilizzo di database privati di riconoscimento facciale da parte delle autorità di contrasto e dei servizi di *intelligence,* come *Clearview AI,* una banca dati di oltre tre miliardi di immagini raccolte illegalmente dai *social network e* da altre fonti di *Internet*»[210].

[208]Cfr., VALLI R.V.O., *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini,* in IL PENALISTA, *2019.*

[209]Cfr., Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale 2020/2016(INI), par. 27.

[210] Cfr., Ivi, par. 28.

In attesa dell'approvazione del Regolamento sulla c.d. legge sull'intelligenza artificiale[211], l'Italia, in via del tutto transitoria, ha approvato una moratoria con la quale, escludendo i rilievi effettuati dalla autorità giudiziaria relativamente alla repressione e prevenzione dei reati, o anche in caso di ottemperanza a sanzioni penali (d.lgs 51/2018) ha ritenuto ammissibili i sistemi biometrici di riconoscimento facciale nei luoghi pubblici fino alla fine del 2023. Nonostante questi correttivi, però, che denotano la volontà dell'Italia di adeguarsi alla normativa europea, nell'ambito della tutela dei diritti fondamentali, è pur vero che, purtroppo, vengono ancora adottate TRF che non sono scevre da critiche, come il Sistema Automatico di Riconoscimento Immagini (SARI) di cui il Ministero dell'interno dispone dal 2017, con funzioni da remoto, denominato, *Enterprise*.

Tramite questo sistema si identifica una persona ''ignota'', da una foto, mediante «una ricerca computerizzata nella banca dati AFIS (*Automated Fingerprint Identification System*), e grazie a due algoritmi di riconoscimento facciale,[SARI *Enterprise*] è in grado di fornire un elenco di immagini, ordinate secondo un grado di similarità»[212].La banca dati AFIS contiene anche un Sotto Sistema Anagrafico (Ssa), nel quale vengono acquisite anche le impronte digitali e le foto segnaletiche presenti nei *database*[213]della polizia, unitamente alle informazioni fisiche delle persone ritratte. Nel settembre 2018, dopo il successo ottenuto nell'identificazione di due persone georgiane accusate di aver commesso un furto, il sistema SARI *Enterprise,* dopo un periodo di sperimentazione, ha ottenuto l'autorizzazione circa il suo utilizzo dal Garante per la protezione dei dati personali»[214]. Ad oggi il sistema è diventato una tecnica utilizzata dalle forze dell'ordine nella lotta alla criminalità.

---

[211]V. artt. a 9 a 12, lg. n. 3374/2021, di conversione del d.l. n. 139/2021.

[212]Cfr., Così si può leggere sul sito del Ministero dell'Interno, *www.interno.gov.it*. Sul tema, in letteratura, v. LOPEZ R., *La rappresentazione facciale tramite* software, in SCALFATI A., *Le indagini atipiche*, GIAPPICHELLI, (a cura di), Torino, 2019, 239 ss.

[213]V., ad es., *Brescia: ladri d'appartamento identificati con il riconoscimento facciale*, 2018, in *www.repubblica.it*.

[214]Cfr., GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Sistema automatico di ricerca dell'identità di un volto, provvedimento n. 440 del 26 luglio 2018.

Il Garante non ha espresso, altrettanto, parere favorevole, nel 2021, relativamente alla modalità *real time* di SARI, ritenendola lesiva dei diritti e delle libertà dei soggetti sottoposti a controllo[215]ed esprimendo una valutazione negativa, del *real time* relativamente alla protezione della *privacy* dei cittadini (DPIA), evidenziando i suoi effetti discriminatori, relativamente all'utilizzo del sistema tattico per monitorare le operazioni di sbarco e le attività illegali compiute dai migranti[216].

Il Garante, ha ritenuto che il riconoscimento facciale, in modalità *real-time*, sia illegale, in quanto «realizza un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che partecipano a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di Polizia»[217]. Ciò determinerebbe, infatti, «una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui»[218].

Il Garante per la protezione dei dati personali, si è pronunciato anche su *Clearview AI*, società che svolge attività di ricerca e trattamento dei dati, utilizzando il TRF, su immagini presenti nel *web*, (tecniche di *web scraping* normalmente vietate), trasferendo poi i detti dati alla pubblica autorità. Il Garante ha espresso parere negativo in quanto ha ritenuto che l'attività svolta dalla software non consiste, "nella mera classificazione di individui sulla base di caratteristiche note, ma nella gestione di dati biometrici che consente un tracciamento nel tempo delle persone ad essi associate"[219]. Inoltre, ha ritenuto la detta acquisizione di dati come distorta, e contraria alle disposizioni del GDPR relative ai principi che devono caratterizzare il trattamento dei dati (di

---

[215]Cfr., COLUCCINI R., *Lo scontro Viminale-Garante sul riconoscimento facciale*, in *IRPI media*, 2020.

[216]V. il report di HERMES, *Centro per la trasparenza e i diritti umani digitali, Tecnologie per il controllo delle frontiere in Italia. Identificazione, riconoscimento facciale e finanziamenti europei*, 2020.

[217]Cfr., GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Parere sul sistema Sari Real Time, provvedimento n. 127 del 25 marzo 202.

[218]*Ibidem.* Per un commento ai provvedimenti del Garante, cfr. anche MOBILIO G., *Tecnologie di riconoscimento facciale*, cit., 240 ss.

[219]*Ibidem.*

correttezza e trasparenza, di limitazione delle finalità e di limitazione della conservazione), condannando la medesima società al pagamento di una sanzione amministrativa pecuniaria nel limite edittale massimo di venti milioni di euro[220] in favore di alcuni soggetti che avevano proposto reclamo al Garante per aver scoperto che la società deteneva immagini, di loro proprietà, che le raffiguravano senza che avessero prestato il consenso.

8. Il riconoscimento facciale: bilanciamento con i diritti fondamentali

Un dibattito sempre aperto è quello relativo al bilanciamento del riconoscimento facciale con il rispetto dei diritti fondamentali. Bilanciamento che non può essere prestabilito dal legislatore, ma deve essere esaminato volta per volta, dall'interprete, in maniera flessibile. Infatti, non esistono criteri oggettivi o matematici per valutare la prevalenza dell'uno sugli altri, ma solo criteri elastici che si fondano sulla proporzionalità, sulla necessità e sulla *extrema ratio*. Più nel dettaglio: la limitazione del diritto fondamentale deve essere proporzionata allo scopo; deve essere dettata da criteri di necessità nel senso che deve essere strettamente necessaria e, infine, deve essere utilizzata se non vi è altro modo per raggiungere un interesse pubblico preminente.

Sul punto sono intervenuti anche la Commissione Europea nel Libro Bianco sull'intelligenza artificiale e il Consiglio d'Europa che hanno elaborato delle Linee Guida relativamente all'uso del riconoscimento facciale[221], affermando che l'utilizzo dell'IA può pregiudicare i valori su cui si fonda l'Unione e rischia di violare diritti fondamentali e di essere discriminatorio relativamente ad elementi come il sesso, la razza, la etnia, la religione e la libertà di pensiero.

---

[220]Cfr., GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Ordinanza ingiunzione nei confronti di CLEARVIEW AI, provvedimento n. 50 del 10 febbraio 2022.

[221]Cfr., Comitato Consultivo della Convenzione 108 (istituito presso il Consiglio d'Europa), *Linee guida sul riconoscimento facciale*, 2021,5 *«The use of live facial recognition technologies in uncontrolled environments, in light of the intrusiveness it bares upon the right to privacy and the dignity of individuals, coupled with a risk of adverse impact on other human rights and fundamental freedoms, should be subject to a democratic debate on its use and the possibility of a moratorium pending complete analysis»*.

Fatta questa premessa, tenendo ben presente il bilanciamento dei diritti fondamentali con l'utilizzo e trattamento dei dati biometrici, passiamo all'esame dettagliato dei singoli diritti fondamentali, strettamente correlati e rapportati allo strumento del riconoscimento facciale.

(i)Il diritto alla tutela della dignità umana.

Il riconoscimento facciale può limitare enormemente la tutela della dignità umana[222], in quanto vengono acquisiti innumerevoli dati che interessano la sfera intima e privata delle persone. Ciò è particolarmente evidente nei casi in cui viene utilizzata una tecnologia cosiddetta *REAL TIME* che è in grado di incamerare innumerevoli dati, spesso neanche attinenti o, addirittura estranei, con lo scopo della ricerca (pericolosità e probabilità di commissione di un reato). Tale acquisizione di dati estranei è illegittima proprio perché lede la dignità delle persone interessate che si vedrebbero ingiustamente controllate anche in ambiti privatissimi.[223].

(ii)Il diritto alla riservatezza e alla protezione dei dati personali.

Il diritto alla riservatezza e alla protezione dei dati[224]la cui tutela è resa difficile dal fatto che molto spesso questi dati vengono raccolti all'insaputa del soggetto interessato e, quindi, senza il suo consenso. Ciò si verifica principalmente nelle aree e nelle manifestazioni pubbliche dove il riconoscimento facciale viene utilizzato senza alcun avvertimento, con la conseguenza che il soggetto perde, inconsapevolmente, il potere di controllo sui propri dati.

(iii)Il diritto all'identità e all'immagine personale.

---

[222]Cfr., La Carta dei Diritti fondamentali dell'Unione Europea all'art 1 enuncia il principio secondo cui «la dignità umana è inviolabile». Il medesimo principio è enunciato all'art. 12 della Dichiarazione Universale dei Diritti dell'Uomo, nonché all'art. 17 del Patto internazionale relativo ai diritti politici e civili. Nell'ordinamento interno, invece, il fondamento normativo del diritto alla tutela della dignità umana è generalmente ritenuto presupposto agli artt. 2 e 3 Cost.

[223]Cfr., Per ulteriori riflessioni sul punto si segnala SORO A., *La protezione dei dati personali nell'era digitale, in Nuova Giur. Civl*, 2019, 2, 343 ss.

[224]Cfr., In assenza di un'espressa previsione normativa, la giurisprudenza ha ricondotto il fondamento normativo di tale diritto agli artt. 2, 13, 14 e 15 Cost., nonché negli artt. 10 c.c. e artt. 96 e 97 della legge sul diritto d'autore (legge 22 aprile 1il soggetto941, n. 633). Tale diritto, invece, trova esplicito fondamento normativo nella Dichiarazione universale dei diritti dell'uomo (art. 12), nel Patto internazionale relativo ai diritti civili e politici (art. 17), nonché nella C.E.D.U. (art. 8). Tra le fonti comunitarie, il diritto alla protezione dei dati personali è espressamente enunciato all'art. 8 della Carta di Nizza, nonché all'art. 16, par. 1, TFUE.

L'attività del trattamento dei dati biometrici si scontra anche col diritto alla tutela della propria identità e immagine personale[225]. È indubbio, infatti, che il dato personale rappresenta un attributo della persona, in quanto rivela elementi che consentono l'identificazione inequivoca di un determinato soggetto[226]. In questo contesto, dunque, il potere di controllare l'attività di trattamento dei propri dati da parte di terzi soggetti rappresenta un nucleo essenziale della tutela della persona umana. Nell'utilizzo dei sistemi di riconoscimento facciale tale potere sembra essere progressivamente marginalizzato.

(iv)Il diritto all'autodeterminazione del soggetto titolare.

L'utilizzo e trattamento dei dati biometrici può costituire una grave violazione del diritto all'autodeterminazione del titolare dei dati[227]. Anche in questo caso, infatti, il soggetto spesso non è al corrente del rilievo dei dati e, quindi, non può esprimere il suo assenso o dissenso in totale autonomia, né viene informato su come i suoi dati saranno utilizzati e conservati. Tale situazione inibisce profondamente il diritto di scelta del soggetto e si pone in netto contrasto con la progressiva valorizzazione che tale diritto ha nel contesto del GDPR; in particolare nella parte in cui si precisa che il soggetto sia sempre al corrente di tutte le «informazioni significative sulla logica utilizzata nel trattamento, sull'importanza e le conseguenze previste per la persona» (art. 14, parag. 2, lett. g).[228].

(v) Il diritto alla tutela giurisdizione e all'equo processo e il diritto di accesso.

[225]Cfr., Il diritto all'identità e all'immagine personale può trovare un suo implicito fondamento costituzionale nella "clausola aperta" di cui all'art. 2 Cost. Tra le fonti primarie, invece, il diritto all'identità e all'immagine personale è espressamente tutelato agli art. 10 c.c., art. 96 co. 1, l. 22 aprile 1941, n. 633.

[226]Cfr., MESSINETTI R., *Circolazione dei dati personali e autonomia privata,* in *Federalismi,* fasc. XXI, 2019, 5.

[227]Il fondamento normativo del diritto all'autodeterminazione è generalmente rinvenuto agli artt. 2 e 21 Cost.

[228]Cfr., COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini,* in SISTEMA PENALE—SP, fascicolo n. IX , 2022, 24 e 27.

Anche in questo caso, il trattamento dei dati biometrici può creare delle disfunzioni in termini di giusto processo[229] e diritto alla tutela giurisdizionale. Infatti, è ormai dimostrato da vari studi[230], quanto sia frequente, principalmente nella fase di prevenzione dei crimini, acquisire notizie da utilizzare nel successivo processo, assolutamente non aderenti alla realtà processuale o addirittura errati. Questi margini di errore compromettono in maniera sostanziale il diritto per cui si discute, in quanto soggetti estranei ai fatti subiscono ingiustamente persecuzioni, imputazioni o peggio ancora ingiusti processi o, ancora, sottoposizioni a misure limitative della libertà personale del tutto inaccettabili.

(vi)Il diritto alla libertà di associazione e alla libertà di manifestazione del pensiero.

A seguito dell'utilizzo di sistemi biometrici, il singolo potrebbe rinunciare alla propria libertà di manifestazione del proprio pensiero e libertà di riunione[231] per non essere inserito in un archivio dati senza il suo consenso Infatti molto spesso, durante le manifestazioni, vengono utilizzati sistemi di riconoscimento facciale, in modalità *REAL TIME* che sono in grado di acquisire innumerevoli dati, tra cui tutte le immagini riguardanti i partecipanti, anche quelli assolutamente incensurati e che sono lì solo per esprimere un loro diritto. Tale consapevolezza comprime e limita la libertà della persona che vede inibito o condizionato il suo diritto a partecipare, e ad esprimere il proprio pensiero per non essere catalogato – ingiustificatamente – negli archivi della Polizia di Stato.

[229]Il diritto alla tutela giurisdizionale e il diritto all'equo processo trovano esplicito fondamento agli artt. 24 e 111 Cost, nonché all'art. 6 C.E.D.U. e ART. 47 Carta di Nizza.

[230]Cfr., COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in SISTEMA PENALE—SP, fascicolo n. IX , 2022, 24 e 27.

[231]Cfr., Autorevole dottrina costituzionalista riconduce le manifestazioni pubbliche all'alveo della libertà di riunione (*ex pluris*, BINR. - PITRUZZELLAG., *Diritto Costituzionale*, in GIAPPICHELLI (a cura di), Torino, 2010. Il diritto della libertà di riunione trova fondamento costituzionale all'art. 17 Cost. È espressamente sancito all'art. 11 C.E.D.U. e art. 12 Carta di Nizza.

CAPITOLO IV

L'IMPATTO DEGLI ALGORITMI SUI DIRITTI FONDAMENTALI DELL'INDIVIDUO

1. L'utilizzo dell'IA nelle attività di *law enforcement* può definirsi etico?

L'utilizzo delle tecnologie di *artificial intelligence* e di analisi dati (*big data systems*) si sono rivelate nelle attività di polizia molto efficaci in alcuni casi in termini di prevenzione e repressione del crimine, in altri hanno creato problematiche relative ad errori di sistema o di identificazione, a pregiudizi discriminatori (*racial bias*), a mancanza di trasparenza circa il meccanismo di funzionamento, alla responsabilità e della privacy. Quest'ultima, in particolare, rischia costantemente di essere violata, in un'ottica futura in cui c'è il pericolo di una ''sorveglianza di massa''[1]. Manca una disciplina specifica ed è fondamentale, quindi, bilanciare l'equilibrio tra diritti degli individui e responsabilità nel campo delle *FRT*[2]e dell'Intelligenza Artificiale (IA) in generale; molte questioni devono, tuttavia, ancora essere risolte.

In particolare, il *focus* principale riguarda l'utilizzo delle TRF, a scopi preventivi-repressivi del crimine e investigativi, da parte delle forze di polizia. È dubbio, infatti, se la forza pervasiva di questi *software*, capace di assorbire quantità ingentissime di dati personali, spesso anche senza il consenso degli interessati, sia compatibile con l'etica o meno.

[1] Si rimanda al Cap. III.

[2]Cfr., ALMEIDA Denise, SHMARKO Konstantin, LOMAS Elizabeth, *The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks*, in AI AND ETHICS (a cura di), 2021, *https://doi.org/10.1007/s43681-021-00077-w.*

Tramite la c.d. *''impact assessment*[3]*''* (la valutazione d'impatto) sulla protezione dei dati (*data protection impact assessments—DPIA*[4]) e sui diritti umani[5] potrebbero trovarsi soluzioni tali da rendere questi sistemi avanzati maggiormente compatibili con la sfera personale degli individui, rendendo il loro uso maggiormente etico. A mezzo della citata valutazione d'impatto sono stati formulate dieci tematiche critiche che devono essere considerate per l'utilizzo degli *Artificial Intelligence Systems* legittimo ed eticamente compatibile:

(i) controllare lo sviluppo autonomo dei *software* di *machine learning*, le modalità di acquisizione dei dati, e il collaudo. Ciò al fine di garantirne la corretta gestione e contrastare il rischio di output pregiudizievoli[6];

(ii) determinare in quali contesti e per quali scopi sia legittima la raccolta di immagini da parte degli *FRT Systems*[7];

(iii) sviluppare consensi informati e avvisi per gli individui che rischiano di essere tracciati[8];

(iv) esplicare, a livello normativo, in quali casi la costruzione e l'utilizzo di banche dati facciali siano legittimi e il fine annesso[9];

(v) programmare la ''scatola nera'' relativa al funzionamento del *''data scraping*[10]*''* della macchina in un'ottica di equità e trasparenza;

(vi) stabilire i limiti[11] relativi all'uso degli *AI Systems*;

(vii) determinare le responsabilità derivante da una cattiva gestione, abusi di utilizzo, o usi diversi[12] da quelli consentiti dalla legge dei sistemi di IA;

---

[3]*Ibidem.*
[4]*Ibidem.*
[5]Cfr., HILL, K., *Activists Turn Facial Recognition Tools Against the Police,* in *The New York Times*, 2020, *https://www.nytim es.com/2020/10/21/technology/facial-recognition-police.html*.
[6] Cfr., ., ALMEIDA Denise, SHMARKO Konstantin, LOMAS Elizabeth, *The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks*, in AI AND ETHICS (a cura di) , 2021, *https://doi.org/10.1007/s43681-021-00077-w.*
[7]*Ibidem.*
[8]*Ibidem.*
[9]*Ibidem.*
[10]*Ibidem.*
[11]*Ibidem.*
[12]*Ibidem.*

(viii) modalità con cui determinare la responsabilità[13], ossia determinare quando finisce la colpa umana e inizia l'errore autonomo della macchina non imputabile all'uomo;

(ix) prevedere le modalità con cui i cittadini possano esporre reclamo[14]o contestare una valutazione algoritmica o l'acquisizione illecita delle loro immagini o delle loro informazioni personali;

(x) infine, valutare se mediante la normazione di un quadro legislativo in materia di IA sia più agevole valutare l'efficacia delle attività di *law enforcement*, i sistemi di controllo, proteggendo, allo stesso tempo, i diritti personalissimi degli individui.

Risolvendo queste questioni, i problemi derivanti dall'uso dell'IA potrebbero essere sensibilmente attenuati.

Tra tutti i sistemi di questo genere, quello maggiormente preoccupante è sicuramente quello del *facial recognition*, a causa della gravissima lesione della privacy che ne deriva.

Occorre, quindi, distinguere gli usi idealmente ''ammissibili' da quelli eccessivamente pervadenti della sfera personale altrui.

L'UE si è pronunciata sul punto più volte, affermando che l'uso delle TRF negli spazi pubblici è significativamente diverso dall'uso, ad esempio, del riconoscimento facciale per lo sblocco dei dispositivi elettronici[15]. Nel primo caso, infatti, senza giustificazione mirata al tracciamento, si rischia di cadere in un regime di sorveglianza di massa, nel secondo, invece, l'uso dell'IA si traduce in una garanzia ulteriore per gli individui di proteggere il contenuto privato dei loro *computer* o *smartphones*, in più, in questo caso, i proprietari dei dispositivi offrono un esplicito consenso al trattamento dei dati facciali.

L'azienda produttrice di software Lenovo, nel 2008, ha infatti, lanciato una nuova serie di *laptop* che, invece di richiedere una password per lo sblocco, utilizzava il riconoscimento del volto dell'utente autorizzato. Questa nuova funzione, sicuramente vantaggiosa a livello di *marketing*, risulta anche legalmente ammissibile, in quanto non contraria alla *privacy* degli individui.

[13]*Ibidem.*
[14]*Ibidem.*
[15]*Ibidem.*

Attualmente questo sistema, infatti, viene utilizzato da quasi tutti coloro che posseggono un *iPhone*, con i modelli di ultima generazione, mentre negli anni passati l'identificazione veniva effettuata mediante le impronte digitali, tramite consensi espressi.

Per cui sussistono rilevanti distinzioni tra l'abbinamento facciale in uno spazio controllato pressoché privato (es. Apple con i volti degli utenti che usufruiscono dello ''sblocco facciale'' o mediante impronte), volto a perseguire vantaggi individuali trasparenti, rispetto all'adozione e all'utilizzo di processi di verifica facciale su larga scala, con annessa acquisizione di *big data*, e per di più senza consenso al trattamento dei dati personali. In altre parole, l'uso dell'IA non è sbagliato o lesivo in senso assoluto, ma dipende al contesto in cui si applica.

Gli sviluppi tecnologici hanno aiutato in modo incomparabile le forze di polizia e le azioni dei servizi segreti o in generale le azioni investigative; tuttavia, è necessario indirizzare gli sviluppatori delle macchine verso un'ottica di trasparenza, di equità, priva di pregiudizi, evitando una distorsione degli input, causa inevitabile di errori sistemici[16]. Una programmazione degli algoritmi predittivi o repressivi del crimine, eticamente compatibile, potrebbe, infatti, condurre a risultati investigativi più efficaci, efficienti e accurati.

Conclusivamente l'IA contiene in sé il potenziale per sfidare i pregiudizi, per elaborare analisi precise e affidabili e per essere utilizzata in modi innovativi ed eticamente compatibili, ma è necessario per questo operare in un'ottica di trasparenza e tentare, quanto più possibile, di evitare distorsioni pregiudizievoli di programmazione che condurrebbero la macchina ad una valutazione ''di parte'' e non neutra come invece si aspira.

Un significativo esempio è quello dell'uso della FRT, avvenuto recentemente, da parte di alcuni attivisti dei diritti umani, che hanno utilizzato le tecnologie facciali per identificare i rischi ''predittivi'' legati all'abuso di

[16] Cfr., BUOLAMWINI J., and GEBRU,T. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, Proceedings of Machine Learning Research*, in *PMLR*, 77 e 91.

potere da parte delle forze dell'ordine mediante questi sistemi[17], ad esempio tramite un controllo di massa dei *social network,* che potrebbe essere paragonato ad una perquisizione perenne senza mandato[18].

Un altro esempio è quello dell'uso delle tecnologie facciali per aiutare, tramite la tecnologia di abbinamento di immagini (*matching*), a identificare le foto o i video originali da quelle false elaborate al computer.

Ne deriva che l'uso delle nuove tecnologie, privato dai suoi aspetti potenzialmente lesivi, può essere di grande aiuto; non è l'utilizzo a crearne la pericolosità, bensì il *modus.*

2.La Carta etica della CEPEJ del Consiglio d'Europa

In data 3 dicembre 2018 la Commissione Europea per l'efficienza della giustizia (CEPEJ) del Consiglio di Europa,[19] ha adottato La "Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi"[20].

La Carta afferma cinque principi, ciascuno dei quali è corredato da una nota esplicativa.

Il primo enunciato è il principio del rispetto dei diritti fondamentali. Nella nota esplicativa si ribadisce il rispetto dei diritti fondamentali, come sanciti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) e dalla Convenzione n. 108 del Consiglio d'Europa, che disciplina la tutela dell'uso abusivo del trattamento automatizzato di dati personali. Con riguardo alle modalità di utilizzo degli strumenti di intelligenza artificiale, inoltre, vengono affermati, con forza, il

[17] Cfr., HILL, K., *Activists Turn Facial Recognition Tools Against the Police,* in *The New York Times*, 2020, *https://www.nytimes.com/2020/10/21/technology/facial-recognition-police.html.*
[18] Cfr., PATTON, D.U. et al , *Stop and frisk online: theorizing every- day racism in digital policing in the use of social media for identification of criminal conduct and associations,* in *Social Media Society*, 2017, *https://doi.org/10.1177/20563 05117733344.*
[19]CEPEJ , 2018, 14
[20]Analizza il contenuto della Carta, focalizzandosi sulle principali questioni relative al settore penale, QUATTROCOLO S., *Intelligenza artificiale e giustizia: nella cornice della carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen.*, 2018.

principio del giusto processo e il principio di legalità, di indipendenza dei giudici e del rispetto del contraddittorio.

Il secondo sancito è il principio di non discriminazione la cui nota esplicativa ribadisce la necessità di evitare l'uso di strumenti di intelligenza artificiale che possano causare o aggravare discriminazioni quali l'origine etnica, le condizioni sociali ed economiche, gli orientamenti politici, religiosi e filosofici. Soprattutto, si chiede agli operatori, che utilizzano le tecniche di intelligenza artificiale, di non adottare *output* derivanti da apprendimenti automatici pregiudizievoli, senza previo controllo, e nell'elaborazione degli algoritmi, di neutralizzare, in partenza, i lamentati effetti discriminatori.

Il terzo principio, di qualità e sicurezza dei dati, prescrive l'utilizzo di dati sicuri, di qualità e di fonti certificate. Per questo, i dati devono essere sottoposti a rigidi controlli da parte dei programmatori per accertare che siano acquisiti, dagli algoritmi, mediante siti validi, di modo che sia garantita l'intangibilità e l'integrità. Importante, se non indispensabile, è che i modelli vengano elaborati con modalità multidisciplinari, a stretto contatto con gli operatori del diritto (professioni legali, ricercatori in materie giuridiche).

La nota esplicativa del quarto principio di trasparenza, imparzialità ed equità sancisce la necessità di rendere le metodologie di trattamento dei dati accessibili e comprensibili, con annesse verifiche esterne, volte ad evitare risultati algoritmici pregiudizievoli e a garantire la corretta applicazione della legge. Il fine è quello di garantire la trasparenza nelle comunicazioni utilizzando un linguaggio chiaro e comprensibile relativo al funzionamento e all'applicazione degli strumenti biometrici.

Il quinto principio di garanzia del controllo umano deve essere applicato per garantire che successivamente al risultato elaborato dalla macchina (output)ci sia un doveroso controllo umano. Quindi il risultato della elaborazione della IA non è di natura prescrittiva dal momento che può essere subordinata o contestata dal controllo degli operatori giudiziari. Oltre ciò il soggetto sottoposto a processo deve essere informato, in maniera chiara, dell'utilizzo di strumenti di intelligenza artificiale, del valore delle elaborazioni algoritmiche nell'ambito del processo penale (ammissibilità/acquisizione della

prova algoritmica) e deve essere informato che può non accettarle e richiedere l'intervento di un Giudice umano. Resta sempre garantita l'assistenza legale.

La Carta, poi, si compone di due appendici.

La prima appendice della Carta[21]esamina i meccanismi di funzionamento degli strumenti di IA e, in tale ottica, evidenzia che quelli che rientrano nella nozione di I.A. debole o moderata non sono attendibili perché, non costituiscono il frutto di un ragionamento umano, ma effettuano una valutazione statistica, elaborando una mole gigantesca di dati; questi tipi di valutazioni, spesso, cagionano, infatti, un alto margine di errore.[22]. Viene poi ribadito il rischio di discriminazione[23], e di lesione della garanzia del giusto processo[24] e del diritto di difesa. Viene affermata la tutela dei diritti fondamentali, della protezione dei dati personali[25], e, in particolare, si richiama il principio di lealtà nel trattamento dei dati, che vieta l'utilizzo di dati per scopi diversi da quelli per cui sono stati acquisiti.

La Carta nella seconda appendice suddivide quattro livelli di cautela correlati all'uso di strumenti di intelligenza artificiale: usi da incoraggiare perché ritenuti privi di rischi[26];possibili utilizzi che esigono notevoli precauzioni tecnologiche; usi da esaminare all'esito di ulteriori studi scientifici; usi da esaminare con le più estreme riserve.

3.La protezione della *privacy* e dei diritti della persona

In Italia la tutela della *privacy* è stata disciplinata solo nel 1996, con la legge n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", elaborata in attuazione della Direttiva 95/46 CE del Parlamento Europeo, emessa in relazione al trattamento dei dati personali e alla libera

[21]Cfr., RONSIN X., LAMPOS V., MAÎTREPIERRE V., *In-depth study on the use of AI in judicial systems, notably AI applications processing judicial decisions and data*, cit.
[22]*Ivi* § 56 ss., spec. § 66, 71.
[23]*Ivi* § 137.
[24]*Ivi* § 138.
[25]*Ivi* § 141 ss.
[26]Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale* (ricerca scientifica Università Roma Tre), Roma, 2020, 138.

circolazione degli stessi. Oggi, la direttiva 95/46/CE è stata abrogata dal Regolamento UE 2016/679 del Parlamento Europeo (GDPR—Regolamento generale sulla protezione dei dati)e dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101.

A livello europeo, quindi, le riforme in materia di *privacy* sono culminate con l'entrata in vigore del GDPR e della LED (*Data Protection Law Enforcement Directive*—Direttiva 2016/680).

Il GDPR stabilisce un quadro normativo che regola il trattamento dei dati personali[27] e fissa, in senso ampio, la definizione di ''dati personali'', il concetto di ''trattamento'' e consente l'esercizio di una serie di diritti agli individui, proprietari o c.d. ''interessati'', quali: il diritto ad accedere ai propri dati personali, compreso quello di rettifica o cancellazione (diritto all'oblio) o deindicizzazione[28].

I dati personali sono definiti, ai sensi dell'art. 3.1 LED e art. 4.1 GDPR, come: «qualsiasi informazione relativa a una persona identificata o identificabile sulla base di tali dati». Nel parere nel 2007 del Gruppo di lavoro articolo 29, un organo consultivo in materia di protezione dei dati costituito ai sensi della direttiva sulla protezione dei dati[29], è stata espressa un'interpretazione del concetto di "dati personali", in senso ampio[30]. (Gruppo di lavoro articolo 29, 2007).

Per ''trattamento'', invece, si intende: «qualsiasi operazione o insieme di operazioni compiute su dati personali o su insiemi di dati personali, anche con mezzi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'utilizzo , divulgazione mediante trasmissione, diffusione o

[27] V., articolo 2, paragrafo 2, GDPR.
[28] V., sent 13 maggio 2014 n. 317 CGUE, (*Google Spain*), in cui vengono sanciti i diritti alla deindicizzazione dei dati e il diritto all'oblio.
[29] Cfr., LYNSKEY Orla, *Criminal justice profiling and EU data protection law: precarious protection from predictive policing, International Journal of Law in Context, in* CAMBRIDGE UNIVERSITY PRESS (a cura di) , 2019, 162–176, 15, 163 e 175.
[30] V., Gruppo di lavoro articolo 29, 2007.

altrimenti messa a disposizione, allineamento o combinazione, restrizione, cancellazione o distruzione» (articolo 3, paragrafo 2, LED e articolo 4, paragrafo 2, GDPR).

A loro volta, i titolari del ‘’trattamento’’, ossia coloro che determinano le modalità e i mezzi di trattamento dei dati personali[31], sono responsabili di un adeguato uso dei dati ai sensi dell’art 5 comma 2 del GDPR e devono rispettare i principi e le garanzie relativi al medesimo trattamento, garantendone la liceità[32].

La materia è stata disciplinata anche nella Carta di Nizza, (Carta dei diritti fondamentali dell'Unione europea) che all’art. 7 prevede il rispetto della vita privata e familiare (*privacy*), mentre l'art. 8 sancisce la tutela dei dati di carattere personale (*data protection*):

(i) Articolo7 Rispetto della vita privata e della vita familiare: ‘’Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni’’. La medesima protezione è altresì confermata dall’art 8 CEDU.

(ii) Articolo8Protezione dei dati di carattere personale: ‘’1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.3. Il rispetto di tali regole è soggetto al controllo di un’autorità indipendente’’.

La Carta di Nizza, originariamente documento politico, è diventata giuridicamente vincolante nel 2007, con il Trattato di Lisbona, entrato in vigore nel 2009, a seguito del quale, tali diritti sono stati riconosciuti diritti fondamentali autonomi e come tali, si è reso necessario regolamentarli in tutti gli Stati dell’Unione; da qui la necessità di un regolamento, applicabile a tutti gli Stati dell'Unione**.**

[31] Cfr., LYNSKEY Orla, *Criminal justice profiling and EU data protection law: precarious protection from predictive policing, International Journal of Law in Context, in* CAMBRIDGE UNIVERSITY PRESS (a cura di) , 2019, 162–176, 15, 163 e 175.
[32] V., articoli 5 e 6 del GDPR.

Il diritto alla tutela dei dati personali trova le sue basi nel diritto al rispetto della dignità della persona umana, che è un diritto fondamentale dell'individuo ed un valore dominante in tutte le carte dei diritti. Da esso discendono il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza.

La tutela dei dati personali è un diritto proprio delle persone fisiche ed è un diritto autonomo, rispetto al diritto alla riservatezza (*privacy*). Mentre la privacy in senso stretto rappresenta un diritto individuale che tutela il singolo da interferenze sulla propria vita privata,(*ius excludendi alios)*, il diritto alla protezione dei dati personali, invece, estende la tutela dell'individuo oltre la sfera della vita privata e in particolare nelle relazioni sociali, così garantendo l'autodeterminazione decisionale e il controllo sulla circolazione dei propri dati (espandendosi nel diritto alla protezione dell'identità personale), contro ogni controllo illegittimo e ogni ingerenza altrui.

Il diritto alla protezione dei dati (*data protection*) è oggetto di grande tutela a causa dell'acquisizione selvaggia degli stessi che viene fatta dalle aziende del web, spesso senza alcun consenso. Per questo motivo sono stati sanciti alcuni principi che regolano l'acquisizione e l'utilizzo dei dati. Tali principi sono: la liceità, correttezza e trasparenza nel trattamento dei dati; la limitazione della finalità, i dati devono, infatti, essere trattati solo per uno scopo legittimo e specifico, oltre che esplicito; la minimizzazione dei dati, che devono essere adeguati, rilevanti e necessari (non eccessivi) rispetto alla finalità; l'accuratezza, che comporta che i dati devono essere mantenuti aggiornati e completi; la limitazione della conservazione, nel senso che i dati devono essere conservati solo per il tempo necessario rispetto alla finalità; l'integrità e confidenzialità, affinché i dati siano trattati in modo sicuro e in modo da non subire alterazioni o accessi non autorizzati[33].

Tornando al Reg. n. 679/2016 (*General Data Protection Regulation*), è necessario chiarire ulteriori elementi. Visto il grave pericolo di lesione derivante dall'uso dei nuovi *AI Systems,* il legislatore europeo ha predisposto uno statuto speciale per proteggere, in modo più rafforzato, alcune categorie

[33] Cfr., PARODI Cesare e SELLAROLI Valentina, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo (DPC)*, fascicolo n. VI, 2019, 59 e 61 .

particolari di dati personali, tra cui: i dati genetici, biometrici e i dati «relativi alla salute»[34]. In particolare, questi ultimi dati comprendono, al loro interno, due tipi di dati: i cc.dd. dati ''immediatamente sensibili'' (o sensibili in senso stretto), ossia quelli che coincidono con lo stato di salute in senso proprio, o come ad esempio le caratteristiche genetiche, il gruppo sanguigno, le risultanze audiometriche, e i cc.dd. dati mediamente sensibili (o sensibili in senso ampio), ossia dati che rivelano profili di c.d. ''intimità'', come ad esempio fragilità quali stato di dipendenza da sostanze stupefacenti, o la comune caratteristica di indossare gli occhiali da vista, caratteristiche, quindi, che pur non essendo strettamente genetiche, mostrano indizi rilevanti su sfere private della persona[35].

Ogni tipo di trattamento sui dati particolarmente sensibili è vietato ai sensi dell'art 9 GDPR, salvo che «per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali» (lett. f) e «per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato» (lett. g).

Proprio su questo punto la normativa in materia di *privacy* si scontra con il funzionamento degli algoritmi predittivi, che si alimentano, per definizione, con ogni tipologia di dati, compresi quelli sensibili o giudiziari[36], perché sono progettati per creare una mappatura della personalità degli individui o *heat maps*. Per cui la presente normativa risulterebbe inadeguata alla protezione delle informazioni oggetto di trattamento algoritmico.

In tal proposito una la sentenza del T.A.R. Lazio, sez. III bis, n. 3769/2017, ha riconosciuto il diritto dell'istante, in qualità di interessato, all'accesso ad un

[34] Cfr., PARODI Cesare e SELLAROLI Valentina, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo (DPC),* VI, 2019, 59 e 61.
[35] *Ibidem.*
[36] In proposito, v. l'art. 10 GDPR, rubricato "Trattamento dei dati personali relativi a condanne penali e reati": «Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, deve avvenire soltanto sotto il controllo.

algoritmo utilizzato dall'amministrazione pubblica nella gestione dei procedimenti di competenza[37].

Tuttavia, spesso, questi sistemi ''artificiali'' sono funzionali alla formazione della prova nel processo penale; in questi casi è più difficile acquisire la prova medesima, garantendo allo stesso tempo la trasparenza, lasciando, così, spazio ad ampi profili di incertezza[38]. Allo stesso tempo,

[37]La sentenza in analisi ha riconosciuto il diritto dell'istante in quanto l'algoritmo, pur essendo preordinato all'esecuzione di doveri stabiliti dalla normativa scolastica, finiva per decidere di fatto quale dovesse essere la destinazione del docente in sede di assegnazione degli istituti scolastici di servizio. In questo senso, il procedimento algoritmico è parte integrante del procedimento amministrativo che dà vita al conseguente atto e, pertanto, rientra nell'alveo dell'accesso agli atti disciplinato dalla legge n. 241/1990. *Cfr.*, sul punto, FORGIONE I., Il caso dell'accesso al software MIUR per l'assegnazione dei docenti – T.A.R. Lazio Sez. III bis, 14 febbraio 2017, n. 3769, in Giornale di diritto amministrativo, 2018, 647 ss.; VIOLA L., *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Foro amm.*, 2018, 1598 ss.; SIMONCINI A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1/2019, 73 ss.

[38]In tema di limiti giuridici all'utilizzabilità della prova, v. infra NOTARO L., ricerca dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica». Con riferimento alla legislazione italiana in materia di privacy, v. anche l'art. 2-octies d.lgs. n. 196/2003 (c.d. Codice della privacy), rubricato "Principi relativi al trattamento di dati relativi a condanne penali e reati": «1. Fatto salvo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del Regolamento, che non avviene sotto il controllo dell'autorità pubblica, è consentito, ai sensi dell'articolo 10 del medesimo regolamento, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati. 2. In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui al comma 1 nonché le garanzie di cui al medesimo comma sono individuati con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante. 3. Fermo quanto previsto dai commi 1 e 2, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare: a) l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del regolamento; b) l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali; c) la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti; d) l'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia; e) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; f) l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia; g) l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza; h) l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto; i) l'accertamento del

nell'ottica della *predictive policing*, gli algoritmi potrebbero essere di grande aiuto per creare, ad esempio, una mappatura che colleghi, per ogni categoria di reato, i corrispondenti elementi costitutivi e preparatori, sia di tipo oggettivo che soggettivo, spesso ripetuti a livello statistico, così da creare, per la polizia, un fascicolo ''preventivo'' per pre-analizzare questi elementi ancor prima della commissione di un qualsiasi reato e quindi prima dell'instaurazione del procedimento e poi del processo. Il principio di economia processuale verrebbe, in questo modo, sicuramente rispettato.

L'uso di questi strumenti, oltre che a livello nazionale, ad ausilio quindi dei governi e delle attività di *law enforcement* dei singoli Stati, potrebbe essere d'aiuto anche in contesti più ampi come ad esempio il contesto europeo. Si pensi, ad esempio, un uso di tali sistemi da parte dell'*Europol* o dell'*EPPO*, ad uso preventivo-repressivo del crimine[39].Tuttavia, secondo il ''*Big Brother Watch*[40]'', un'organizzazione del Regno Unito, sussiste una tendenza crescente delle forze dell'ordine dell'UK ad ''acquisire, sviluppare, o incrementare'' l'uso di tecnologie invasive di polizia predittiva, di dubbia compatibilità con i diritti fondamentali e il loro esercizio e garanzia. Queste attività di polizia comprendono: ''una grande varietà di tecniche utilizzate dai dipartimenti di

requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti; l) l'attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese ai sensi dell'articolo 5-ter del decreto-legge 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla legge 24 marzo 2012, n. 27; m) l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo. 4. Nei casi in cui le disposizioni di cui al comma 3 non individuano le garanzie appropriate per i diritti e le libertà degli interessati, tali garanzie sono previste con il decreto di cui al comma 2. 5. Quando il trattamento dei dati di cui al presente articolo avviene sotto il controllo dell'autorità pubblica si applicano le disposizioni previste dall'articolo 2-sexies. 6. Con il decreto di cui al comma 2 è autorizzato il trattamento dei dati di cui all'articolo 10 del Regolamento, effettuato in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata, stipulati con il Ministero dell'interno o con le prefetture-UTG. In relazione a tali protocolli, il decreto di cui al comma 2 individua, le tipologie dei dati trattati, gli interessati, le operazioni di trattamento eseguibili, anche in relazione all'aggiornamento e alla conservazione e prevede le garanzie appropriate per i diritti e le libertà degli interessati. Il decreto è adottato, limitatamente agli ambiti di cui al presente comma, di concerto con il Ministro dell'interno».

[39]Sull'apertura del diritto alle altre scienze e alla necessità di condivisione dei saperi, cfr. GARBOLINO P., *Nuovi strumenti logici e informatici per il ragionamento giudiziario: le reti bayesiane*, in Cass. pen., 1/2007, 326 ss.

[40] V., *U.K. Parliament, Home Affairs Select Committee: Policing for the Future Inquiry*, in *Big Brother Watch*, 2018

polizia per generare e agire in base alle probabilità di crimine (valutazione del rischio delle persone[41]), spesso indicate come previsioni[42]''.

L'utilizzo dell'IA può essere, quindi davvero efficace, ma va sfruttato in modo lecito, e controllato, onde evitare il rischio di abusi, motivo per cui la normativa europea valuta l'applicazione di tali sistemi in modo molto restrittivo e mai affidando agli algoritmi la completa autonomia di accedere senza sosta e limiti ai dati personali, a maggior ragione se su larga scala, con la annessa pericolosità di ledere i diritti degli individui, e di sfuggire completamente al controllo umano.

3.1 Le previsioni rilevanti nell'ambito del *data protection reform package*dell'UE: la Direttiva UE/2016/680 e il divieto di decisioni esclusivamente automatizzate

Il Regolamento UE 679/2016 e la Direttiva 2016/680 hanno disciplinato la materia relativa alla protezione dei dati personali all'interno dell'Unione Europea.

In particolare, l'art. 11 della Direttiva 2016/680[43], disciplina il trattamento dei dati da parte delle «Autorità competenti per le attività di polizia, di indagine e accertamento dei reati e di esecuzione delle sanzioni penali».

---

[41] Cfr., OSWALD M et al. , *Algorithmic risk assessment policing models: lessons from the Durham HART model and 'experimental' proportionality,* in *Information & Communications Technology Law*, 2018, 223-250, 27.

[42] Cfr., DEGELING M *and* BERENDT B *What is wrong with Robocops as consultants? A technology-centric critique of predictive policing, In AI & Society*, 2018, 347-356, 33.

[43] Articolo 11 («Processo decisionale automatizzato relativo alle persone fisiche»):
«1. Gli Stati membri dispongono che una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato sia vietata salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento.
2. Le decisioni di cui al paragrafo 1 del presente articolo non si basano sulle categorie particolari di dati personali di cui all'articolo 10, a meno che non siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato.
3. La profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 10 è vietata, conformemente al diritto dell'Unione».

La direttiva in esame, nel primo paragrafo, vieta gli Stati membri a formulare decisioni ‘’basate unicamente su un trattamento automatizzato’’, qualora producano effetti giuridici negativi o incidano significativamente sulla sfera personale dell’interessato[44]. Tali decisioni possono essere adottate solo mediante disposizioni *ad hoc* dell’Unione o dello Stato membro cui è sottoposto il titolare del trattamento, a patto che non siano violati i suoi diritti e libertà fondamentali, e non gli sia precluso il diritto di richiedere di adire il giudice, in quanto “decisore umano”[45].

La Direttiva, al secondo paragrafo, vieta le decisioni basate sul trattamento automatizzato dei dati sensibili (previsti dall’art. 10 del Regolamento). Trattamento automatizzato che però può essere adottato, nel caso in cui vengano adottate idonee misure a tutela dell’interessato.

Nel terzo paragrafo la Direttiva pone l’assoluto divieto di attività di ‘’profilazione’’ qualora queste si basino su dati sensibili e producano effetti discriminatori nei confronti di persone fisiche.

Posto il dato normativo, appare necessario interpretare il divieto di adottare una «decisione basata unicamente su un trattamento automatizzato»[46],

[44]Un divieto di analogo tenore è previsto, con ambito di applicazione più generale, all’art. 22 del Regolamento UE 2016/679 («Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione»):
«1. L’interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l’esecuzione di un contratto tra l’interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell’interessato; c) si basi sul consenso esplicito dell’interessato.
3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell’interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d’applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato». Si può ricordare, peraltro, che un divieto di decisioni basate unicamente su trattamenti automatizzati era già previsto dall’art. 15 della Direttiva 95/46/CE.
[45] Cfr., GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale* (ricerca scientifica Università Roma Tre), Roma , 2020, 142.
[46] Cfr., GIALUZ M., *Quando la giustizia penale incontra l’intelligenza artificiale*, cit., 16.

esaminandone i limiti ed i parziali correttivi, dal momento che detta espressione appare abbastanza ambigua[47].

La regola base, come abbiamo visto, esclude l'ammissibilità delle decisioni basate esclusivamente alla valutazione di una macchina. Tuttavia, pare sia consentito utilizzare l'intelligenza artificiale come supporto, a condizione che vi sia una valutazione sostanziale della decisione[48] da parte dell'operatore umano che giammai deve autenticare e sottoscrivere la decisione della macchina in maniera simbolica[49] o automatica, ed inoltre l'output elaborato dalla macchina, può essere utilizzato come indizio, da utilizzare ed integrare con altri elementi di prova.[50].

In buona sostanza, si ammette una deroga al posto divieto, a condizione che siano sufficientemente tutelati i diritti della persona e vi sia un intervento umano, di modo che la decisione dell'intelligenza artificiale sia valutata anche da altre fonti. L'interessato, poi, conserva il diritto di richiedere la pronuncia

---

[47] Con riguardo alla previsione analoga contenuta nell'art. 22 GDPR, si legga LA DIEGA G. N., A*gainst the Dehumanisation of decision-Making. Algorithmic decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, in *JIPITEC*, 2018, 18 s.

[48]Cfr. BRKAN M., *Do algoritms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond*, in *Electronic Journal, 2017, 10: «In order for the decision not to be based solely on automated processing, the human judgment needs to be such as to verify the machine-generated decision and the human should assess the substance of the decision and not be involved merely as another (empty) procedural step. In other words, in order to escape the prohibition from Article 22 GDPR or Article 11 of the Directive on Data Protection in Criminal Matters, the human has to use the machine only as decision support, whereas the final decision is taken by the human»*. In senso analogo, cfr. le linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 (17/IT; WP 251 rev.01), 23, nella versione emendata adottata il 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione dei dati, istituito dall'art. 29 della direttiva 95/46/CE: «Il titolare del trattamento non può eludere le disposizioni dell'articolo 22 creando coinvolgimenti umani fittizi. Ad esempio, se qualcuno applica abitualmente profili generati automaticamente a persone fisiche senza avere alcuna influenza effettiva sul risultato, si tratterà comunque di una decisione basata unicamente sul trattamento automatico. Per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico. Il controllo dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza per modificare la decisione. Nel contesto dell'analisi, tale persona dovrebbe prendere in considerazione tutti i dati pertinenti»

[49] *Linee guida sul processo decisionale automatizzato,* cit., 23. Vi deve essere un «*meaningful and genuine human intervention, for instance in the form of actual oversight by a person with "authority and competence to change the decision"»* LA DIEGA G.N., *Against the Dehumanisation of decision-Making,* cit., 19.

[50]Cfr., GIALUZ M., *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., 16; MALGIERI G,. COMANDÈ G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law,* vol. VII, 2017, 14; MANES V., *L'oracolo algoritmico e la giustizia penale*, cit., 20.

di una persona fisica, che dovrà prendere in considerazione e valutare elementi di prova ulteriori rispetto a quelli elaborati dalla macchina.

Quanto al divieto di cui al paragrafo 3, occorre specificare che la LED definisce la profilazione come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, la preferenze, interessi, affidabilità, comportamento, posizione o movimenti[51]».

Se, come suggerito in precedenza, i sistemi di polizia predittiva comportano il trattamento di dati personali, ne consegue che tali sistemi sono sistemi di "profilazione" in quanto prevedono aspetti relativi all'affidabilità e al comportamento di una persona fisica nonché potenzialmente alla sua ubicazione e ai suoi spostamenti. La profilazione è di per sé quindi una forma di processo decisionale automatizzato (gruppo di lavoro articolo 29, 2017)[52].

In buona sostanza, le regole sancite a livello europeo, se da un lato, cercano di salvaguardare l'IA, dall'altro ne vietano fermamente l'utilizzo quando l'impiego dei *tools*, produca effetti discriminatori.

CONCLUSIONI

[51] V., art. 3(4) LED; art. 4, (4) GDPR.
[52]Cfr., ., LYNSKEY Orla, *Criminal justice profiling and EU data protection law: precarious protection from predictive policing, International Journal of Law in Context, in* CAMBRIDGE UNIVERSITY PRESS (a cura di) , 2019, 162–176, 15, 163 e 175 .

All'esito dell'analisi sin qui compiuta, possiamo ritenere che nei prossimi anni l'Intelligenza Artificiale assumerà un ruolo ancor più centrale nelle dinamiche economiche, sociali, politiche e giuridiche. Ciò impone sin da subito agli interpreti di confrontarsi con il tema spinoso del bilanciamento dei rischi-benefici del suo utilizzo, soprattutto in riferimento alla giustizia e alla tutela dei diritti costituzionalmente garantiti all'individuo.

Infatti, come si è ampiamente descritto nel corso dell'elaborato, l'IA è una tecnologia in rapido sviluppo, ed è nata per evolversi sempre di più mediante il c.d. autoapprendimento; ma se da un lato è uno strumento di grossa utilità, dall'altro solleva importanti questioni etiche e giuridiche circa la dubbia imparzialità e trasparenza delle decisioni dalle macchine e i relativi impatti sulla *privacy*. Non si deve dimenticare, infatti, che la raccolta costante di dati personali, soprattutto se effettuata all'oscuro degli individui crea difficili questioni da risolvere, oltre alla difficoltà di individuare una disciplina applicabile per la tutela di queste informazioni.

In aggiunta, l'applicazione degli strumenti di intelligenza artificiale al campo della giustizia potrebbe ''snaturare'' o ''deumanizzare'' alcune attività giuridiche che fondano le loro basi sulla soggettività della decisione, la quale, certamente, non può essere rimessa al mero calcolo elaborato da una macchina, incapace di ponderare elementi prettamente psicologici ed emozionali tipici dell'essere umano. Queste circostanze, come già detto, destando grosse perplessità, conducono innumerevoli studiosi a contrastare uno sviluppo dell'intelligenza artificiale incontrollato. Occorre infatti, per un corretto uso di questi sistemi, un costante controllo umano, ad esempio mediante la supervisione di un ente governativo in grado di monitorare l'autonomia algoritmica e limitarne l'applicazione. In tal senso si mira in Italia e in Europa allo sviluppo di una normativa *ad hoc*. Naturalmente, l'intento non è quello di fermare lo sviluppo dell'IA, ma di elaborare una disciplina specifica che regoli la materia e che fissi in maniera chiara i principi etici e i regimi di responsabilità; i limiti e le condizioni per il ricorso all'Intelligenza Artificiale; il divieto di applicazioni altamente invasive dei diritti fondamentali e della privacy; l'eliminazione delle discriminazione fondate su pregiudizi; la garanzia di sistemi di sorveglianza umana attivabili immediatamente in caso di necessità; i limiti, in

termini di validità, delle risposte date dalle macchine e basate esclusivamente su dati statistici (ciò, in quanto se le macchine vengono programmate male o, in maniera condizionata dai pregiudizi dell'operatore, il rischio di risposte sbagliate diviene molto alto), dal momento che, non si può anteporre all'uomo l'algoritmo, ma occorre regolamentare e verificare l'uso dei dati, per avere risultati sicuri ed affidabili, a tutela dei diritti fondamentale dei cittadini.

In sintesi, se da un lato è indubbio che i sistemi di IA sono molto utili relativamente alla rapidità della raccolta dei dati e dei i procedimenti, dall'altro suscitano molte perplessità concernenti il raffronto con i diritti fondamentali e con la certezza del diritto (nonché, rispetto alle applicazioni processuali, con i principi del giusto processo). Pertanto, la valutazione della utilizzabilità nel sistema penale della tecnologia algoritmica non può essere generalizzata in positivo o in negativo, dovendo essere contestualizzata caso per caso, in rapporto ai diversi ambiti di applicazione.

In definitiva, quello che fa la differenza è sempre la capacità di controllo e di validazione umana, per evitare pericolose disfunzioni. Non è l'uso dell'IA in sè pericoloso ma il *come*.

BIBLIOGRAFIA

ACKERMAN Spencer, *FBI Quietly Changes Its Privacy Rules for Accessing NSA Data on Americans*, in *GUARDIAN*, 2016.

ADAMS Guy, *The Sci-Fi Solution to Real Crime*, in *Independent*, Londra, 2012, 32.

AHLSTROM, WINTON, and HAVIGHURSTRobert J. (1982). "*The Kansas City Work/Study Experiment.*" in SAFER DANIEL J., (a cura di), *School Programs for Disruptive Adolescents. Baltimore, Maryland: Univer- sity Park Press*.

AHUMADA Rosalio, *Modesto Sees Double-Digit Drop in Property Crimes-Lowest in Three Years*, in *Modesto Bee*, 2014.

ALDAX Mike, *Richmond Police Chief Says Department Plans to Discontinue "Predictive Policing" Software*, in *Richmond Standard*, 2015.

ALETRAS N., TSARAPATSANIS D., PREOTIUC-PIETRO D., AND LAMPOS V., *Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective*, in *Peer J Computer Science*, 2016, 1 ss., 11 ss.

ALKHATIB Ali et al., *On Recent Research Auditing Commercial Facial Analysis Technology*, in *Medium*, 2019, *https://medium.com/@bu64dcjrytwitb8/on-recent-research-auditing-commercial-facial-analysis-technology-19148bda1832, [https://perma.cc/ W7SJ-38P2*].

ALMEIDA Denise, SHMARKO Konstantin, LOMAS Elizabeth, *The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks*, in AI AND ETHICS (a cura di), 2021, *https://doi.org/10.1007/s43681-021-00077-w.*

ANDREWS, D.A., ZINGERI., HOGE R.D., BONTAJ., GENDREAUP., and F.T.,"*Does Correctional Treatment Work? A Clinically Relevant and a Psychologically Informed Meta-Analysis*." In *Criminolog*,1990, 28:369–404.

ANGWIN J., KIRCHNER L., LARSON J., MATTU S., *Machine Bias*, in *www.propublica.org*, 2016.

ANGWIN Julia, *Dragnet nation: a quest for privacy, security, and freedom in a world of relentless surveillance*, 2014, 3.

ANSELIN Luc et al, *Mbasurement and analysis of crime and justice* ,2000, 213 e 215.

ANSELIN Luc et al., *Spatial Analyses of Crime*, in *4 Criminal Justice*, 2000.

AOL Digital Justice, *Digisensory Technologies Avista Smart Sensors*, 2012, available at *www.youtube.com/watch?v=JamGobiSswg*; Associated Press, NJ City Leading Way in Crime-Fighting Tech, in *CBSNEWS*, 2010, *www.cbsnews.com*.

ARAMINI, M. *I processi inferenziali nel profilo psicologico del criminale* in *Psicologia&Giustizia*, 2002, 1, 2 s.

ASHBY Andrew, *Operation Blue CR.U.S.H. Advances at Mpd*, in *Memphis daily NEWS*, 2006, *http://www.memphisdailynews.com/editorial/Article.aspx?id=30029*, C.R.U.S.H.(Crime Reduction Using Statistical History) (diretto da).

ASLAM Salman, *Facebook by the Numbers: Stats, Demographics & Fun Facts*, in *Omnicore*, 2020, *https://www.omnicoreagency.com/facebook-statistics* [*https://perma.cc/936W -4Z9G*].

AUSTEN Ben, *Public Enemies: Social Media Is Fueling Gang Wars in Chicago*, in *Wired*, 2013, *https://www.wired.com/2013/09/gangs-of-social-media* [*https:// perma.cc/MD29-DC4N*].

BAILEY Ronald, *Stopping Crime before It Starts*, in *Reason*, 2012, *http:// reason.com*.

BARBASCHOW Asha, *How One Sheriff's Office Is Using Machine Learning to Uncover Persons of Interest*, in *ZDNET*, 2017, *https://www .zdnet.com/article/how-one-sheriffs-office-is-using-machine-learning-to-uncover -persons-of-interest [https://perma.cc/L9RY-NE3F]*.

BAROCAS Solon & SELBST Andrew D., *Big Data's Disparate Impact*, in *Calif.*, 2016, 671, 683–684, 104.

BASILE F., *Intelligenza artificiale e diritto penale, quattro possibili percorsi di indagine*, cit., 10 ss., 22 ss , 32 s.

BASILE Fabio, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in*DPU-DIRITTO PENALE E UOMO*, 2019, Fascicolo 10, 16 ss., 22 ss.

BAXTER Stephen, *Modest Gains in First Six Months of Santa Cruz's Predictive Police Program*,in S*antacruz Sentinel*, 38 e 50.

BEAM Christopher, *Time Cops: Can Police Really Predict Crime before It Happens*?, In *Slate*, 2011, *www.slate.com.*

BECK Charlie &MCCUE Colleen, *Predictive Policing: What Can We Learn from Wal-Mart and Amazon About Fighting Crime in a Recession?*, in *Police Chief*, 2009, 18.

BEHN Robert D., *The PerformanceStat Potential: a Leadership Strategy for Producing Results*, 2014.

BEISER Vince, *Forecasting Felonies: Can Computers Predict Crimes of the Future*?, in *Pacific Standard*, 2011, 20, *http://psmag.com*.

BENJAMIN RUHA, *Race after technology: abolitionist tools for the new jim code* , 2019, 109.

BERK Richard, HEIDARI Hoda, JABBARI Shahin, KEARNS Michael & ROTH Aaron, *Fairness in Criminal Justice Risk Assessments: The State of the Art*, in *Socio. Methods & Sch.*, 12 e 15, *https://arxiv.org/pdf/1703.09207.pdf, [https://perma.cc/W86U-9DP7*].

BERMAN Jules J., *Principles of big data: preparing, sharing, and analyzing complex information*,2013, 2.

BERNASCO Wim, *Them Again? Same-Offender Involvement in Repeat and Near Repeat Burglaries*, in *Eur. J. Criminol*,2008, 411-412, 5;

BIDGOOD Jess, *After Arrests, Quandary for Police on Posting Booking Photos*, in *N.Y.TIMES*, 2015.

BINR. – PITRUZZELLA G., *Diritto Costituzionale*, in GIAPPICHELLI (a cura di), Torino, 2010.

BIVENS *v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, in *U.S.*, 1971, 388-392, 403.

BLOCK Robert, *Requests for Corporate Data Multiply: Businesses Juggle Law-Enforcement Demands for Information about Customers, Suppliers*, in *WALL ST. J.*, 2006, A4.

BONDY Halley, *East Orange Installs Surveillance Cameras That Sense Criminal Activities, Alerts Police*, in *Star- Ledger*, Newark, 2010, *www.nj.com*.

BORSARI R., *Intelligenza Artificiale e responsabilità penale: prime considerazioni*, in *www.medialaws.eu*, 2019,2, 3.

BOYD Aaron, *ICE Outlines How Investigators Rely on Third-Party Facial Recognition Services*, in *Nextgo*, 2020, *https:// www.nextgov.com/emerging-tech/2020/06/ice-outlines-how-investigators-rely-third-party-facial-recognition-services/165846 [https://perma.cc/SL4J-DHUK]*.

BRAGA Anthony A., HUREAU David M., & PAPACHRISTOS Andrew V., *The Relevance of Micro Places to Citywide Robbery Trends: A Longitudinal Analysis of Robbery Incidents at Street Corners and Block Faces in Boston*, in *J. Res. Crime &Delinq.*, 2011, 48, 7 e 9.

BRANDOM, *Police are using facial recognition the wrong way. And altering our faces?*, in *www.theverge.com*, 2019;

BRANTINGHAM Jeffrey, *http:// paleo.sscnet.ucla.edu.*

BRAYNE Sarah, *Stratified Surveillance: Policing in the Age of Big Data*, 2015, 9 e 13.

BRAYNE Sarah, *The Criminal Law and Law Enforcement Implications of Big Data*, in *Ann. rev. l. & Soc. sci.* , 2018, 293-294, 14.

BRESS Jessica, *Policy Advosor at DC Department of Behavioral Health, Presentation, Final Analysis del SBIRT Pilot Program 30/05/2015—02/08/2015.*

BRIDGE, *Police make first arrest using facial recognition surveillance cameras at Cardiff Millennium stadium*, in *www.thetimes.co.uk*, 2017.

BRKAN M., *Do algoritms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond*, in *Electronic Journal, 2017, 10.*

BROKAW Leslie, *Predictive Policing: Working the Odds to Prevent Future Crimes*, *Mitsloan Management Rev.*, 2011, *http://sloanre-view.mit.edu.*

BUOLAMWINI Joy, *How I'm Fighting Bias in Algorithms*, in *Ted*, 2016, *https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms* [*https://perma.cc/32RE-CAYQ*].

BOULAMWINI Joy, *Opinion, When the Robot Doesn't See Dark Skin*, in *N.Y. Times*, 2018, *https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html [https://perma.cc/UV8U-YV93*].

BUOLAMWINI Joy, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, in *Time*, 2019, *http://time.com/5520558 artificial-intelligence-racial-gender-bias, [https://perma.cc/9USJ-K94C*].

BUOLAMWINI Joy, *Response: Racial and Gender Bias in Amazon Rekognition— Commercial AI System for Analyzing Faces*, in *Medium*, 2019, *https://medium .com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced [https://perma.cc/U2F3 -LT4T]*

BUOLAMWINI Joy, *When AI Fails on Oprah, Serena Williams, and Michelle Obama, It's Time to Face the Truth*, in *Medium*, 2018, *https://medium.com/@Joy.Buolamwini/when-ai-fails-on-oprah-serena-williams-and-michelle-obama-its-time-to-face-truth-bf7c2c8a4119, [https://perma.cc/AQC8-PQES*].

BUOLAMWINI Joy & GEBRU Timnit, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, Proceedings of Machine Learning Research*, 2018, in *PMLR*, 77 e 91.

BUOLAMWINI Joy & GEBRU Timnit, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proc. Mach. Learning Rsch*, 2018, 1,11, 81, *http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, [https://perma.cc/Z2XX-GSB3*].

BUOLAMWINI Joy & GEBRU Timnit,, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*; *Concerned Researchers, On Recent Research Auditing Commercial Facial Analysis Technology*, in *www.medium.com*, 2019.

BUOLAMWINI JOY, ORDÓÑEZ VICENTE, MORGENSTERN JAMIE & LEARNED ERIK MILLER, *Facial recognition technologies: a primer*, 2020, 8 ss, *https://global-uploads.webflow.com/5e027cal88c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf [https://perma.cc/X8CH-JAV3]*.

BURCHARD C., *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen*., 2019, 1908 ss., 4.

BURDI Jerome, *Police Looking to Predict Crimes in Palm Beach County*, in *Palm Beach Sun Sentinel*, 2011, *http://articles.sun-sentinel.com/2011-10-30/news/fl-predictive-policing-20111030_1_violent- crime-police-stake-police-agencies.*

BURT Chris, *Motorola Could Offer Facial Recognition with Police Body Cam- eras with WatchGuard Acquisition*, in *Biometric Update*, 2019, *https://www.biometricupdate.com/201907/motorola-could-offer-facial-recognition-with-police-body-cameras-with-watchguard-acquisition [https://perma.cc/6RQG-EHGP]*.

BUSHWICK Sophie, *How NIST Tested Facial Recognition Algorithms for Racial Bias*, in *Sci. Am*., 2019, *https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias* [*https://perma.cc/9JFT-GV22*] .

CAGLE Matt & OZER Nicole A., *Amazon Teams Up with Law Enforcement To Deploy Dangerous New Face Recognition Technology*, in *ACLU N. CAL*., 2018, *https://www.aclunc.org/blog/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology [https://perma.cc/WYF4-7XDT*].

CANDELLI C., CARABELLESE F., ROCCA G., ROSSETTO I., *La valutazione psichiatrico forense della pericolosità sociale del sofferente psichico autore di reato: nuove prospettive tra indagine clinica e sistemi attuariali,* in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario),* 2012, n. 4, 1442 ss., 18.

CANTÚ Aaron, *#Followed: How Police across the Country Are Employing Social Media Surveillance*, in *MUCKROCK*, 2016.

CANZIO, *Il dubbio e la legge*, in *Diritto penale contemporaneo*, 2018, 3 s.

CAPLAN J.M., KENNEDY L.W., *Risk Terrain Modeling: Crime Prediction and Risk Reduction***,** in UNIV. OF CALIFORNIA PRESS (a cura di), 2016**.**

CAPLAN J.M., KENNEDY L.W., BARNUM J.D., PIZAE.L, *Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis to Explore the Dynamics of Criminogenic Behavior Setting*, in *Journal of Contemporary Criminal Justice*, 33, 2017,133 ss.

CARBONI K., *La più controversa startup di riconoscimento facciale sta collaborando con l'Ucraina*, 2022, in *www.wired.it.*

CAREY Camille & SOLOMON Robert A., *Impossible Choices: Balancing Safety and Security in Domestic Violence Representation*, in *CLINICAL*, 2014, 201-225, 21.

CARLO S., *Face off. The lawless growth of facial recognition in UK policing*, in *Big Brother Watch,* 2018.

CARRER L., *La Russia usa il riconoscimento facciale su chi manifesta contro la guerra*, 2022, in *www.wired.it.*

CARRER S., *Se l'amicuscuriae è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin,* in *Giur. pen. web*,2019.

CARTHY J. MC, MINSKYM.L., ROCHESTER N., SHANNONC.E., *A Proposal for the Dartmouth SummerResearch Project on Artificial Intelligence*, 1955, disponibile in *www-formal.stanford.edu*.; 11 KAPLAN J., *Intelligenza artificiale,* cit., 2017, 19.

CASADY Tom, *Police Legitimacy and Predictive Policing,* in *Geography &Pub.Safety*, 2011, 1.

CASTELLETTI L., RIVELLINI G., STRATICÒ E., *Efficacia predittiva degli strumenti di Violence Risk Assessment e possibili ambiti applicativi nella psichiatria forense e generale italiana,* in *Journal of Psychopathology,* 2014, 153 ss.

CASTELLI C. – PIANA C., *Giustizia predittiva. La qualità della giustizia in due tempi*, in *questionegiustizia.it*.

CAVALIERE Victoria, *More Than 100 Indicted in Harlem in Largest-Ever NYC Gang Bust*, in *REUTERS*, 2014), *https://www.reuters.com/article/us-usa-crime-gangs/more-than-100-indicted-in-harlem-in-largest-ever-nyc-gang-bust-idUSKBN0EF1DQ20140604.*

CEVOLANI G. – CRUPI V., *Come ragionano i giudici: razionalità, euristiche e illusioni cognitive, in Criminalia*, 2017, 181 ss.

CHAINEY Spencer & RATCLIFFE Jerry, *Gis and crime mapping*, 2005, 8.

CHAINEYSpencer, TOMPSONLisa, &UHLIG Sebastian, *The Utility of Hotspor Mapping for Predicting Spatial Patterns of Crime*, in *Security J.*, 21 4, 5.

CHAMMAH Maurice, *Policing the Future*, in *The Marshall Project*, 2016, *www.themarshallproject.org*.

CHANDRAN, *Mass surveillance fears as India readies facial recognition system*, in *www.reuters.com*, 2019.

CHICON KERRY, *N.Y. county district att'y's off., intelligence-driven prosecution.*

CHINOY Sahil, Opinion, *The Racist History Behind Facial Recognition*, in *N.Y. times*, 2019, *https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html, [https://perma.cc/DP34-4MWR*].

CHOHLAS-WOOD Alex *is the current director of analytics at the Office of Management Analysis and Planning, New York Police Department.*

CHRISTOPHER BEAM, *Time Cops: Can Police Really Predict Crime Before It Happens?*, in *Slate*, 2011, *http://www. slate.com/articles/news_and_politicscimet2Ol 1/01/time cops.single.html*; *Weekend Edition Saturday*, in *National Public Radio broadcast*, 2011, *http://www.npr.org/2011/11/26/142758000/at-lapd-predicting-crimes-before-they-happen* .

CITRON Danielle Keats, *Spying Inc.*, in *WASH. & LEE*, 2015, 1243-1272, 72.

CITRON Danielle Keats &PASQUALE Frank, *Network Accountability for the Domestic Intelligence Apparatus*, in *HASTINGS*, 2011, 1441-1451, 62.

CITRON Danielle Keats & PASQUALE Frank A., *The Scored Society: Due Process for Automated Predictions,* in *Wash*, 2014, 1, 89.

CLARKE M., *Framing the Xinjiang emergency: colonialism and settler colonialism as pathways to cultural genocide?*, in ID. (a cura di), *The Xinjiang emergency Exploring the causes and consequences of China's mass detention of Uyghurs*, 10 ss.

CLARKE Roger, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, in *Info. Tech. & people*, 1994, 6, 34, 7;

CLARKE Ronald V. and FELSON Marcus, eds., *Routine Activity and Rational Choice, New Brunswick*, in *H.J. Transaction Publishers*, 2003, (*criminal behavior theories*).

CLARRIDGE Christine, *Protesters Steal the Show at Seattle Police Gathering to Explain Intended Use of Drones*, in *SEATTLE TIMES*, 2012.

COHEN Julie E., *What Is Privacy For?,* in *HARV,* 2013, 1904-1920-1921, 126.

COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema Penale —SP*, 2022, 9, 30 ss.

COLDEWEY D., *This facial recognition system tracks how you're enjoying a movie*, in *TechCrunch*, 2017.

COLLINS, *Facial recognition: Do you really control how your face is being used?*, in *eu.usatoday.com*, 2019.

COLONNA Liane, *A Taxonomy and Classification of Data Mining*, in *SMU ScI.&TECH.*, 2013, 309-314 ,16.

COLUCCINI R., *Lo scontro Viminale-Garante sul riconoscimento facciale*, in *IRPI media*, 2020.

CONGER K., FAUSSET R. and KOVALESKI S. F., *San Francisco Bans Facial Recognition Technology*, in *The New York Times*, 2019.

COOK Cynthia M., HOWARD John J., SIROTIN Yevgeniy B., TIPTON Jerry L. & VEMURY Arun R., *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, in INST. ELEC. & ELEC. ENG'RS TRANSACTIONS ON BIOMETRICS, BEHAV. & IDENTITY SCI. (a cura di), 2019, *https:// ieeexplore.ieee.org/document/8636231 [https://perma.cc/5HB5-HAT2*].

COOKE Kristina e SHIFFMAN John, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, in *REUTERS*, 2013.

CORLEY Cheryl, *When Social Media Fuels Gang Violence, all tech considered* in *NPR radio broadcast*, 2015.

COSTANZI C., *La matematica del processo*, in *DPC—Diritto Penale Contemporaneo*, 2014, 234.

COUCHMAN Hannah, *Artificial Intelligence: what it is and why you should care*, in *Liberty*, 2017, *www.libertyhumanrights.org.uk*.

COUCHMANH., *Policing by Machine. Predictive Policing and the Threat to Our Rights*, in *www.libertyhumanrights.org.uk*,2019.

CRAWFORD Kate, *Think Again: Big Data*, in *FP*, 2013, *www.foreignpolicy.com.*

CRAWFORD K., *Né intelligente né artificiale, Bologna,* 2021 cit., 144.

CRAWFORD K., *Né intelligente né artificiale. Il lato oscuro dell'IA*, Il Mulino, Bologna, 2021, p. 119 ss.

CRAWFORD Kate & SCHULTZ Jason, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, in *B.C.*, 2014, 55, 93 s, 104 s.

CROW, W.J., and BULL J.L. (1975). *Robbery Deterrence: An Applied Behavioral Science Demonstration—Final Report. La Jolla, California: Western Behavioral Sciences Institute, and "The Buddy System: Effect of Community Intervention on Delinquent Offenses*.", in *BEHAVIOR THERAPY*, (a cura di), 1975, 522–524.

CUKIER Kenneth, *Data, Data Everywhere,* in *ECONOMIST*, 2010.

CURRAO Elettra, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *DPU—Diritto Penale Uomo*,2021, 2 ss.

CUSHING Tim, *Detroit Police Chief Says Facial Recognition Software Involved in Bogus Arrest Is Wrong '96 Percent of the Time*, in *Techdirt,* 2020, *https://www.techdirt.com/articles/20200629/17423944814/detroit-police-chief-says-facial-recognition-software-involved-bogus-arrest-is-wrong-96-percent-time.shtml [https://perma.cc/9FC8-H2QU*].

DAVENPORT Thomas H., *How Big Data Is Helping the NYPD Solve Crimes Faster,* in *Fortune*, 2016.

DAVEY Monica, *Chicago Has Its Deadliest Month in About Two Decades*, in *N.Y. Times*, 2016.

DAVEY Monica, *Chicago Police Try to Predict Who May Shoot or Be Shot,* in *N.Y. Times*, 2016.

DEARDEN, *Police used facial recognition technology lawfully, High Court rules in landmark challenge*, in *www.independent.co.uk*, 2019.

DEGELING M *and* BERENDT B *What is wrong with Robocops as consultants? A technology-centric critique of predictive policing, In AI & Society*, 2018, 347-356, 33.

DELLA CAVA Marco*, California Could Become First to Limit Facial Recognition Technology; Police Aren't Happy*, in *USA Today*, 2019, *https:// www.usatoday.com/story/news/nation/2019/06/16/california-could-limit-how-police-use-facial-recognition-technology/1456448001 [https://perma.cc/9AZS-8P5F*] .

DELLA TORRE Jacopo, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice,* in *Dirtto Penale Contemporaneo—DPC*, fascicolo n. 1, 2020, 232 e 236.

DEVICH Malkia-Cyril, *Defund Facial Recognition*, in *Atlantic*, 2020, *https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771[https://perma.cc/9P29-JD63]*.

Di GIOVINE O., *Il judge-bot e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale*), in Cass. pen., 2020, 3, 951 ss.

DI GENNARO, G., MARSELLI R.,LOMBARDO E., SPINA M. *Tolleranza zero o deterrenza selettiva*, in DI GENNARO G. e MARSELLI R. (a cura di), 2018;*Secondo Rapporto Criminalità e Sicurezza a Napoli*, in FEDOA PRESS (a cura di), University Federico II, Napoli.

DI NICOLA A, ESPA G, BRESSAN S, DICKSON M, NICOLAMARINO A, *Metodi statistici per la predizione della criminalità. Rassegna della letteratura su predictivepolicing e moduli di data mining.*, 2014.

DOMINGOS Pedro, *The master algorithm: how the quest for the ultimate learning machine will remake our world*, 2015.

DONOHUE Laura K., *Bulk Metadata Collection: Statutory and Constitutional Considerations*, in *HARV.* e *PUB. POL' Y.*, 2014, 757-825, 37.

DONOHUE Laura K., *Technological Leap, Statutory Gap, and Constitutional Abyss:* SEP *Remote Biometric Identification Comes of Age*, in *MINN.*2012, 407-413-435, 97.

DOUGLAS Jason & OLSONParmy, *London Police to Start Using Facial Recognition Cameras*, in *Wall St.J.*, 2020, *https://www.wsj.com/articles/london-police-to-start-using-facial-recognition-cameras-11579895367* [*https://perma.cc/ A3AZ-DARA*].

DRESSEL J., FARID H., *The accuracy, fairness, and limits of predicting recidivism,* in *Science Advances,* 2018, 4, 1 ss.

DUBAL, *San Francisco was right to ban facial recognition. Surveillanceis a realdanger,* in *The Guardian,* 2019.

DUHIGG Charles, *How Companies Learn Your Secrets*, in *N. Y. TIMES MAG.*, 2012.

EAD., *When the Robot Doesn't See Dark Skin*, in *www.nytimes.com*, 2018.

EBERHARDT Jennifer, *Social psychological answers to real- world questions*in *STANFORDSPARQ*, 2016, 12.

EBERHARDT Jennifer, *Strategies for Change: Research Initiatives and Recommendations to Improve Police-Community Relations in Oakland, Calif.*

ENGLICH B.– MUSSWEILER T. – STRACK F., *Playing Dice With Criminal Sentences: The Influence of Irrelevant Anchors on Experts' Judicial Decision Making, in Personality and Social Psychology Bulletin,* 2006, 4, 194.

EUBANKS VIRGINIA, *Auto- mating inequality 37*, 2018.

FARIVAR Cyrus, *Meet Visual Labs, a Body Camera Startup That Doesit Sell Body Cameras*, in *Arstechnica*, 2016, *http://arstechnica.com.*

FERGUSON A. G., "*Predictive Policing" and the Fourth Amendment*, in *Am. Crim.*, 2011, *http://www.americancriminallawreview.com/Drupal/blogs/blog-entry/"predictive-policing"-and-fourth- amendment*-11-28-2011.

FERGUSON A. G., *Predictive Policing and Reasonable Suspicion,* in *EMORY*, 2012, 62, 259-265 ss, ,317.

FERGUSON A. G.,, *Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards*, in *OKLA*,2014, 831-841, 66.

FERGUSON A. G.,, *Big Data and Predictive Reasonable Suspicion*, in *U.PA.*, 2015, 327-370, 163;

FERGUSON A. G., *Predictive Prosecution,* in *WAKE FOREST*, 2016, 720–721, 51,

FERGUSON A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* New York, 2017.

FERGUSON A. G., *Big Data's Watchful Eye: The Rise of Data Surveillance*. In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 2017,7 e 19, in *NYU Press*, 8 s., 37 s, 63 ss. ,71, 89, 124 s. *https://doi.org/10.2307/j.ctt1pwtb27.4.*

FERGUSON A. G.,, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. in *Nyu Press*,2017, 7 s., 69 s., 113, 181.

FERGUSON A. G., *Illuminating Black Data Policing*, in 15 Ohio St. J. Crim. L. 2018, 505, 503 s, 510 ss 523.

FERGUSON A. G., *ACS Central Science Virtual Issue on Machine Learning,*in *ACS Cent. Sci. Publications*, Vol. IV (8), 2018, Washington, StatiUniti, 938.

FERGUSON A. G., *Facial Recognition and the Fourth Amendment*, 2019. In *Minnesota Law Review,* 2021, 1105, 109, 118, 162, 169, 193 *https://ssrn.com/abstract=3473423* or *http://dx.doi.org/10.2139/ssrn.3473423*.

FERGUSON A. G, *Predictive Policing Theory*: *The Cambridge Handbook of Policing in the United States,* in TAMARA RICE LAVE & ERIC J. MILLER CAMBRIDGE UNIV. PRESS (a cura di), 2019, Capitolo 24, American University, WCL Research Paper, 2020-10-496,*https://ssrn.com/abstract=3516382*.

FERGUSON A. G., *Big data prosecution and brady UCLA law review*, vol. LXVII, 2020, 180, 185, 189 s.,203,205 ss., 256.

FERGUSON A. G. & LOGAN Wayne A., *Policing Criminal JusticeData*, in *MINN.*, 2016, 541- 554, 101.

FINGAS Jon, *Chicago Police See Less Violent Crime After Using Predictive Code*, in *Engadget*, 2017.

FLEISHER Tim, *Officers Embrace New Smartphones as Crime Fighting Tools*,

FLORES v. A., BECHTEL K., LOWENKAMP C., False Positives, False Negatives, and False Analyses: A Rejoinder to "*Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*", in *Federal Probation Journal*, 2016

FO, W.S.O., and O'DONELLC.R., "*The Buddy System: Relationship and Contingency Conditioning in a Community Intervention Program for Youth With Non- professionals as Behavior Change Agents.*", in *JOURNAL OF CONSULTING AND CLINICAL PSYCHOLOGY,*1974, 163–69.

FORD Paul, *What is Code?*,in *BLOOMBERG BUSINESSWEEK*, 2015.

FORGIONE I., Il caso dell'accesso al software MIUR per l'assegnazione dei docenti – T.A.R. Lazio Sez. III bis, 14 febbraio 2017, n. 3769, in Giornale di diritto amministrativo, 2018, 647 ss.;

FOX Jeremy C., *Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect*, in *Bos. Globe*, 2019, *https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html, [https:// perma.cc/RZK4-WVXD*]

FRANCE Lisa Respers, *Taylor Swift Reportedly Used Facial Recognition to Try to ID Stalkers*, in *CNN*, 2018, *https://www.cnn.com/2018/12/13/entertainment/taylor-swift-facial-recognition/index.html [https://perma.cc/F9PW -NMQ3].*

FREEMAN K., *Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights* in *State v. Loomis, in North Carolina Journal of Law & Technology*, Vol. XVIII, 2016,75 ss.

FRIED Ina, *Clearview Brings Privacy Concerns from Facial Recognition into Focus*, in *Axios*, 2020, *https://www.axios.com/clearview -facial-recognition-law-enforcement-ac069290-b83e-4934-a9f0-0b782af82588.html [https://perma.cc/X4S6-QJFG];*

FUSSEY e MURRAY D., *Independent Report on the London Metropolitan Police Service's*, cit., 49;

FUSSEY e MURRAY, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, in HUMAN RIGHTS CENTRE, UNIVERSITY OF ESSEX, (diretto da);

GALTERIO Mary Grace, SHAVIT Simi Angelic & HAYAJNEH Thaier, *A Review of Facial Biometrics Security for Smart Devices*, in *MDPI Computers* 2018, 37, 3, 7;

GALTERIO Mary Grace, SHAVIT Simi Angelic & HAYAJNEHT haier, *A Review of Facial Biometrics Security for Smart Devices*, *MDPI Computers* 2018, 3 SS, 37.

GANSLER Douglas F., *Implementing Community Prosecution in Montgomery County,*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Parere sul sistema Sari Real Time, provvedimento n. 127 del 25 marzo 202.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Sistema automatico di ricerca dell'identità di un volto, provvedimento n. 440 del 26 luglio 2018.

GARAPON A., LASSÈGUE J., *Justice Digitale. Révolution graphique et rupture anthropologique*, Paris, 2018.

GARRETT B. L. – MONAHAN J., *Judging Risk, in California Law Review, Forthcoming*, 2020, 10 s.

GARVIE Clare, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, in *GEO. CTR. ON PRIVACY & TECH.*, 2019, *https://www.flawedfacedata.com.*

GARVIE Clare & FRANKLE Jonathan, *Facial-Recognition Software Might Have a Racial Bias Problem*, in *Atlantic*, 2016, *https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991*, [*https://perma.cc/4L5J -AXR4*].

GARVIE CLARE, BEDOYA ALVARO M. & FRANKLE JONATHAN, *GEORGETOWN* in *Priv. & Tech., The perpetual line-up: unregulated police face recognition in America*, 2016, 12, *https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technol-ogy%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/S48P -PL53*].

GARVIE e FRANKLE, *Facial-Recognition Software Might Have a Racial Bias Problem*, in *www.theatlantic.com*, 2016.

GARVIE e MOY, *America under watch,* 2016, in https://www.americaunderwatch.com/.

GARVIE, BEDOJA, FRANKLE, *The perpetual line-up. Unregulated police face recognition in America*, in *https://www.perpetuallineup. org/*, 2016.

GARVIE Clare & MOY Laura, *America Under Watch: Face Surveillance in the United States*, in *Geo. Ctr. on priv. & tech.: am. under watch*, 2019, *https:// www.americaunderwatch.com [https://perma.cc/P6RF-56EB*].

GASSAWAY Brigitte et al., *Engaging the Community: Operation Heat Wave*, in *Geography &Pub.Safety*, 2011, 8 s.

GERMAIN Thomas, *How a Photo's Hidden 'Exif' Data Exposes Your Personal Information*, in *Consumer reps*, 2019, *https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data [https://perma.cc/YPG7-54AS*].

GERMAIN Thomas, *How a Photo's Hidden 'Exif' Data Exposes Your Personal Information*, in *Consumer Reps*, 2019, *https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data* [*https://perma.cc/YPG7-54AS*].

GERSHGORN Dave, *Carnival Cruises, Delta, and 70 Countries Use a Facial Recognition Company You've Never Heard of*, in *Medium: One zero*, 2020, *https://onezero.medium.com/nec-is-the-most-important-facial-recognition-company-you've-never-heard-of-12381d530510 [https://perma.cc/6BDD-E8WJ]*.

GHANI Rayid, intervista di CORNISH Audie, *Can Big Data Help Head Off Police Misconduct?, ALL TECH CONSIDERED* in *NPR radio broadcast,* 2016.

GIALUZ Mitja, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *DPC-Diritto Penale Contemporaneo*, 2019, 11 s, 16.

GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale,* RICERCA SCIENTIFICA UNIVERSITÀ ROMA TRE *(*a cura di*)* , Roma, 2020, 16.

GIRALDI Angelo, GROSSI Lorenza, MASSARO Antonella, NOTARO Laura, SORBELLO Pietro, *Intelligenza artificiale e giustizia penale,* RICERCA SCIENTIFICA UNIVERSITÀ ROMA TRE *(*a cura di*)* , Roma, 2020, 22ss, 57, 65, 138,.

GOEL Sharad et al., *Combatting Police Discrimination in the Age of Big Data*, in *NEW. CRIM.*, 2017, 6, 27.

GOLDBERG Erica, *Getting Beyond Intuition in the Probable Cause Inquiry*, in *Lewis &Clarkl*, 2013, 789 s, 17.

GOLDSTEIN Joseph, *Police Take on Family Violence to Avert Death*, in *N. Y. TIMES*, 2013.

GOLDSTEIN Joseph & GOODMAN J. David, *Seeking Clues to Gangs and Crime, Detectives Monitor Internet Rap Videos*, in *N.Y. Times,* 2014, *https://www.nytimes.com/2014/01/08/nyregion/seeking-clues-to-gangs-and-crime-detectives-monitor-internet-rap-videos.html,* [*https://perma.cc/E2FC-XYN9*] .

GOLDSTEIN Joseph, *F.B.I. Audit of Database That Indexes DNA Finds Errors in Profiles*, in *N.Y. TIMES*, 2014, A15;

GOODE Erica, *Sending the Police before There's a Crime*, in *N. Y. Times*, 2011; *Predictive Policing: Don't Even Think about It*, in *Economist*, 2013, 24 e 26.

GOODMAN J. David, *Dozens of Gang Suspects Held in Raids in Manhattan*, in *N.Y. TIMES*, 2014.

GORDON Michad, *CMPD's Goal: To Predict Misconduct before It Can Happen*, in *CHARLOTTE OBSERVER*, 2016.

GORDON Leslie A., *Predictive Policing May Help Bag Burglars- but It May Also Be a Constitutional Problem*, in *A.B.A.J.*, 2013, *www.abajournal.com*.

GORNER Jeremy, *The Heat List*, in *Chi. Trib.*, 2013.

GROSS Allie, *Experts: Duggan's Denial of Facial Recognition Software Hinges on 3 Words*, in *Det. Free press*, 2019, *https://www.freep.com/story/news/local/michigan/detroit/2019/07/16/duggan-war-of-words-surveillance-tech/1701604001 [https://perma.cc/9N2H-U7HW*]

GROSSMAN Lev et al., *The 50 Best Inventions of the Year*, in *Time*, 2011, 55 e 82.

GROTHER PATRICK, NGAN MEI & HANAOKA KAYEE, *Nat'l inst. standards & tech., internal rep. 8280, face recognition vendor test (frvt) part 3: demographic effects*, 2019, 2 s., *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf*, [*https://perma.cc/4VEW-SD7F*].

GROTHER, NGAN, HANAOKA, *Face Recognition Vendor Test (FVRT). Part 3: Demographic Effects,https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf*, p. 2 e ss;

HACKETT Chris & GROSINGER Michael, *The Growth of Geofence Tools within the Mapping. Technology Sphere*, in *Pdv wireless*, 2014, *www.pdvwireless.com*.

HAMANN e SMITH, *Facial Recognition Technology: Where Will It Take Us?*, in *www. americanbar.org*;

HARCOURT Bernard E. &MEARES Tracey L., *Randomization and the Fourth Amendment*, in *U. CHI.* 2011, 809-862, 78, 210.

HARMON Amy, *As Cameras Track Detroit's Residents, a Debate Ensues over Racial Bias*, in *N.Y. Times*, 2019, *https://www.nytimes.com/2019/07/08/us/ detroit-facial-recognition-cameras.html [https://perma.cc/B5L2-9MS7*].

HARMON Rachel, *Why Do We (Still) Lack Data on Policing?*, in *MARQ.*,2013, 1119-1129, 96.

HARRIES Keith, *Natl Inst. of Justice, mapping crime: principle and practice*, 1999, 92 e 94;

HARWELL Drew, *Oregon Became a Testing Ground for Amazon's Facial- Recognition Policing. But What if Rekognition Gets It Wrong?*, in *Wash. post*, 2019, *https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police [https:// perma.cc/LA3C-JD8K]*.

HELD Myka & MCLAUGHLIN Juliana, *Rape & Sexual Assault*, in *GENDER GEO. J. & L.*, 2014, 155-157, 15.

HETEY Rebecca C. et al, *Data, for Change: A Statistical Analysis of Police Stops, Searches, Hand cuffings, and Arrests in Oakland, Calif*, in *STANFORDSPARQ* 2013-2014.

HETEY Rebecca C. *SOCIAL PSYCHOLOGICAL ANSWERS TO REAL- WORLD QUESTIONS*, 2016.

HILL Kashmir, *The Secretive Company That Might End Privacy as We Know It*, in *N.Y. Times*, 2020, *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, [https://perma.cc/G895 -W3LJ*].

HILL Kashmir, *Wrongfully Accused by an Algorithm*, in *N.Y. Times,* 2020, *https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html, [https://perma.cc/458E-SR99*].

HILL, K., *Activists Turn Facial Recognition Tools Against the Police,* in *The New York Times*, 2020, *https://www.nytimes.com/2020/10/21/technology/facial-recognition-police.html*.

HILL, *New Jersey Bars Police From Using Clearview Facial Recognition App,* in *www.nytimes.com,* 2020.

HILL, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, in *www.nytimes.com,* 2020,

HOBSON Will, *Overhaul Coming to Pinellas Gang Intelligence Database*, in *TAMPA BAY TIME*, 2013, *http://www.tampabay .com/news/courts/criminal/overhaul-coming-to-pinellas-gang-intelligence -database/2125725.*

HOFF Sam, *Professor Helps Develop Predictive Policing by Using Trends to Predict, Prevent Crimes*, in *Daily Bruin*, 2013, *http://dailybruin.com*.

HOGGINS, *'Racist and sexist' facial recognition cameras could lead to false arrests*, in *www.telegraph.co.uk*.

HOLDER Eric, *Community Prosecution*, in *PROSECUTOR*, 2000, 31 s.

HOLT Kris, *Facial Recognition Linked to a Second Wrongful Arrest by Detroit Police*, in *Engadget,* 2020, *https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.htm,l [https://perma.cc/KS46-YWGW]*.

HOWELL K. Babe, *Gang Policing: The Post Stop-and-Frisk Justification for Profile-Based Policing,* in *U.DENV.CRIM*, 2015, 1-15-16, 5.

HSU Spencer S., *FBI Notifies Crime Labs of Errors in DNA Match Calculations Since 1999*, in *WASH. POST*, 2015.

HU Margaret, *Biometric ID Cybersurveillance*, in *IND*, 2013, 1475-1478, 88.

HUNT Priscilla, SAUNDERS Jessica, &HOLLYWOOD John S., *Evaluation of the shreveport predictive policing experiment*, in *RandCorp,*2014, available at *www.rand.org*.

HUROWITZ Noah, *NYPD Terrorism Boss Blasts Council Surveillance Oversight Bill as 'Insane,' DNAINFO*, 2017**,**

IASELLI M., *X-LAW: la polizia predittiva è realtà*, in *Wired.it,*2019;

ISTRIANI E., *Algorithmic Due Process: Mistaken Accountability and Attribution in State v. Loomis*, in *Harvard JOLT Digest*, 2017.

IVANOVA Irina, *Why Face-Recognition Technology Has a Bias Problem*, in *CBS news*, 2020, *https://www.cbsnews.com/news/facial-recognition-systems-racism-protests-police-bias, [https:// perma.cc/Q7ZU-4R33*].

JACKSON J.L., BEKERIAN, D.A., *Does offender profiling have a role to play*, in JACKSON J. L., BEKERIAN, D. A. (diretto da), *Offender profiling: Theory, research and practice, Chichester*, in WILEY (a cura di), 1997, 1 e 7.

JANSEN Bart, *America's Terrorist Watchlist Explained*, in *USA TODAY*, 2016.

JEE Charlotte, *London Police's Face Recognition System Gets It Wrong 81% of the Time*, in *Mit Tech. rev.*, 2019, *https://www.technologyreview.com/201907/04/134296/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time,* [*https://perma.cc/X4J6-TL3V*].

JEROME Joseph W., *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, in *STAN*, 2013, 47-50, 66.

JIE XU ET AL., RUTGERS CTR. ON PUB. SEC., C*rime generators for shootings in urban areas: a test using conditional locational interdependence as an extension of risk terrain modeling*, 2010, 1.

JOH Elizabeth E., *Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion*, in *ARIZ.*, 2013, 997-1002, 55.

JOH Elizabeth E., *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, in HARV. L. & POL'Y, 2016, 10, 115-116, 15.

JOH Elizabeth E., *The Undue Influence of Surveillance Technology Companies on Policing*, in *N.Y.U L. REV. ONLINE*, 2017, 19-20, 92. *https://www.nyulawreview.org/wp-content/uploads/2017/08/NYULawReviewOnline-92-Joh_0.pdf, [https:// perma.cc/AX4Z-TGGR*]; MITTELSTADT Brent, RUSSELL Chris &WACHTER Sandra, *Explaining Explanations in AI*, CONF. ON FAIRNESS, ACCOUNTABILITY & TRANSPARENCY 2019, 279.

JOH Elizabeth E., *Policing by Numbers: Big Data and the Fourth Amendment*, in *WASH.*, 2014, 35-42, 89.

JOHNSON Shane D. et al., *Space-Time Patterns of Risk: A Cross National Assessment of Residential Burglary Victimization*, in *J. Quant. Criminol*,2007, 181ss, 125, 201-203 s, 223.

JOSHI Jagdish Chandra & GUPTA K.K., *Face Recognition Technology*: A Review, in *Jup j. Telecomms* 2016, 53 s, 59, 8.

JOUVENAL Justin, T*he New Way Police Are Surveilling You: Calculating Your Threat "Score"*, in *Wash. post*, 2016.

KALLURI Pratyusha, *Don't Ask If Artificial Intelligence Is Good or Fair, Ask How It Shifts Power*, in *Na-ture*, 2020, *https://www.nature.com/articles/d41586-020-02003-2* [*https://perma.cc/N9MY-M8G9*]

KAMINSKI Margot E., *Regulating Real- World Surveillance*, in *Wash.*, 2015, 1113 -1153,90.

KAPLAN J., *Intelligenza artificiale*, cit., 2017, 19.

KAPLANJ., *Intelligenza artificiale. Guida al futuro prossimo*, in LUISS UNIVERSITY PRESS, (a cura di) 2017, 74 ss. ;

KAYE David H., *Rounding Up the Usual Suspects: A Legal and Logical Analysis of DNA Trawling Cases*, in *N.C.*2009, 425-439, 87;

KAYSER-BRIL, *At least 10 police forces use face recognition in the EU, Algorithm Watch reveals*; in *https://algorithmwatch.org/en/story/face-recognition-police-europe/.*

KEHL D. – GUO P. – KESSLER S., *Algorithms in the Criminal Justice System,* cit., 11.

KELLY Heather & LERMAN Rachel, *America Is Awash in Cameras, a Double-Edged Sword for Protesters and Police*, in *Wash. Post*, 2020, *https://www .washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters [https://perma.cc/F4GX-XDBJ*].

KENNEDY L.W., CAPLAN J.M., PIZAE.L, *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**.**

KENNEDY Leslie et al., R*utgers ctr. on pub. sec., a multi-jurisdictional test of risk terrain modeling and a place-based evaluation of environmental risk-based patrol deployment strategies,* 2015.

KENNEDY Leslie W. et al., *Risk Clusters, Hotspots, andSpatial Intelligence: Risk TerrainModeling as an Algorithm for Police Resource Allocation Strategies*, in *Quantitative Criminology*, 2011, 339, 345-46, 27

KIFT Paula H. e NISSENBAUM Helen, Metadata in Context: *An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program*, in *ISJLP*, 2017, 13.

KING T., AGGARWAL M., TADDEO M., FLORIDI L., *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions,* in *Science and Engineering Ethics Ethics,* 2019, 1 ss.;

KLAYMAN v. Obama (Klayman I), 957 F. Supp. 2d 1, 41 (D.D.C. 2013); *Am. Civil Liberties Union v. Clapper*, 959 F. Supp. 2d 724, 752, S.D.N.Y. 2013.;

KRAJICEK David J., *What's the Best Way to Weed Out Potential Killer Cops*?, in *AITER-NET*, 2016.

KROLL Joshua A. et al., *Accountable Algorithms*, in *U. PA.*, 2017, 633-679-80, 165.

LA DIEGA G. N., A*gainst the Dehumanisation of decision-Making. Algorithmic decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, in *JIPITEC*, 2018, 18 s.

LEARNED-MILLER ERIK, ORDÓÑEZ VICENTE, MORGENSTERN JAMIE & BUOLAMWINI JOY, *Facial recognition technologies in the wild: a call for a federal office*, 2020, 3 s., *https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/ 5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf* [*https://perma.cc/ 5BGG-ML6V*].

LEE Timothy B., *Detroit Police Chief Cops to 96-Percent Facial Recognition Error Rate*, in *Arstechnica,* 2020, *https://arstechnica.com/tech-policy/2020/06/detroit-police-chief-admits-facial-recognition-is-wrong-96-of-the-time, [https://perma.cc/DX2G-986E*].

LEE D., *San Francisco is first US city to ban facial recognition,* in *BBC News,* 2019 *;*

LEE Jeaeh, *Can Data Predict Which Cops Are Most Likely to Misbehave in the Future?* , in *MOTHER JONES*, 2016.

LEIGH Johanna M., DUNNETT Sarah J., and JACKSON Lisa M., *Predictive Policing Using Hotspot Analysis*, Hong Kong, 2016.

LERMAN Jonas, *Big Data and Its Exclusions*, in *STAN* ,2013, ONLINE S,57s, 66.

LEVASHOV Kirill, *The Rise of a New Type of Surveillance for Which the Law Wasn't Ready*, in *Colum. Sci. & Tech*. 2013, 15, 164, e 167 ss.

LEVINSON Rachel -*Waldman, Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, in *EMORY,*2017, 527-534, 66.

LI e CADELL, *China eyes "black tech" to boost security as parliament meets*, in *www.reuters.com,* 2018.

LIND Dara, *Turning the No Fly List into the No Gun List Explained*, in *VOX*, 2016, *www.vox.com*;

LIPP Kenneth, *AT&T Is Spying on Americans for Profit, New Documents Reveal*, in *DAILY BEAST*, 2016.

LITHWICK Dahlia e VLADECK Steve, *Taking the "Meh" out of Metadata*,in *SLATE*, 2013.

LOCKLEAR Mallory, *DHS Will Use Facial Recognition To Scan Travelers at the Bor-der*, in *Engadget ,* 2018, *https://www.engadget.com/2018/06/05/dhs-facial -recognition-scan-travelers-at-border [https://perma.cc/V4E8-7N7M]*.

LOGAN Wayne A., *Knowledge as power: criminal registration and community notification laws in America*, 2009, 178 – 81.

LOGAN Wayne A., *Police Mistakes of Law,* in *EMORY*, 2011,69-90–92,61.

LOGAN Wayne A. &WRIGHT Ronald F., *Mercenary Criminal Justice,* 2014,1175.

LOGAN Wayne A., *Database Infamia: Exit from the Sex Offender Registries*, in *WIS*, 2015, 219.

LOGAN Wayne A., *Government Retention and Use of Unlawfully Se- cured DNA Evidence*, in *TEX. TECH*, 2015, 269-280, 48.

LOGAN Wayne A. &FERGUSON Andrew Guthrie, *Policing Criminal Justice Data,* inFSU COLLEGE OF LAW (diretto da), Minnesota, 2016 , Law Review 541, Research Paper n. 799, 559.

LOHR Steve, Amid the Flood, *A Catchphrase Is Born*, in *N.Y. TIMES,* 2012.

LOHR, *Facial Recognition Is Accurate, if You're a White Guy*, in *www.nytimes.com,* 2018.

LOMAS Natasha, *London's Met Police Switches on Live Facial Recognition, Flying in the Face of Human Rights Concerns*, in *Techcrunch,* 2020, *https:// techcrunch.com/2020/01/24/londons-met-*

police-switches-on-live-facia -recognition-flying-in-face-of-human-rights-concerns [*https://perma.cc/Y9QR-L7E6*];

LOPEZ, *La rappresentazione facciale tramite software*, SCALFATI A., *Le indagini atipiche*, in GIAPPICHELLI (a cura di), Torino, 2019, 239 ss, 244.

LOW Arnold H., *Rethinking Search and Seizure in a Post-911 World*, in *MISS.*, 2011, 1507-1518, 80.

LUM K., *Predictive Policing Reinforces Police Bias, in Human Rights Data Analysis Group*.

LUM, K. ISAAC W., *To predict and serve?*, in *Significance*, 2016, 10vol. XIII, 14 e 19;

LYNCH J., *Face Off Law enforcement use of face recognition technology* in *Social Science Research Network*, 2020.

LYNSKEY Orla, *Criminal justice profiling and EU data protection law: precarious protection from predictive policing, International Journal of Law in Context, in* CAMBRIDGE UNIVERSITY PRESS (a cura di), 2019, 162–176, 15, 163 e 175.

LYNSKEY Orla, *Criminal justice profiling and EU data protection law: precarious protection from predictive policing, International Journal of Law in Context, in* CAMBRIDGE UNIVERSITY PRESS (a cura di), 2019, 162–176, 15, 163 e 175 .

LYON D., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, in FELTRINELLI (a cura di), Milano, 2002, 2.

MAASS Dave e MACKEY Aaron, *Law Enforcement's Secret "Super Search Engine" Amasses Trillions of Phone Records for Decades*, in *ELECTRONIC FRONTIER FOUNDATION*, 2016.

Madeline Purdue, *Axon Body-Camera Supplier Will Not Use Facial Recognition in Its Products – For Now*, in *USA today*, 2019, 2:17 PM, *https://www.usatoday.com/story/tech/2019/07/01/axon-rejects-facial-recognition-software-body-cameras -now/1601789001 [https://perma.cc/324C-AALN]*.

MAJORITY Staff of S. Comm. on Commerce, Sci., & Transp., Office of Oversight & Investigations, *A review of the data broker industry: collection, use, and sale of consumer data for marketing purposes*, 2013, 5 e 8. available at *www.commerce.senate.gov*

MALGIERI G,. COMANDÈ G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, vol. VII, 2017, 14.

MALY Tim, *Anti-Drone Camouflage: What to Wear in Total Surveillance*, in *WIRED*, 2013, *www.wired.com*.

MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, *in Intelligenza artificiale*. Il diritto, i diritti, l'etica, in RUFFOLO U. (a cura di), 2020, 547 ss.

Manhattan district att'y's office, models for innovation: the Manhattan district attorney's office 2010–2018, 2018, 19 50 ss.

MANTOVANI R., *Digital Life, Il supermercato ti riconosce dalla faccia*, in *Focus*, 2017.

MARGULIES Peter, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection after Snowden*, in *HASTINGS*, 2014, 1, 51-57, 66 ;

MARTINEZ Michael, *Policing Advocates Defend Use of High-Tech License Plate Readers*, in*CNN*, 2013, *www.cnn.com.*

Maryland, in *PROSECUTOR*, 2000, at 30, 30–31.

MASSARO A., *Determinatezza della norma penale e calcolabilità giuridica*, in EDITORIALE SCIENTIFICA (a cura di), 2020, 494.

MASTROBUONI G., *Crime is Terribly Revealing: Information Technology and Police Productivity*, 2014, 2741-2753.

MASTROBUONI G., (*Lead Academic*) *Impact: Imagine being able to predict a crime in the future*, *Research case study by University of Essex*, in *www.essex.ac.uk*, 2021.

MASTROBUONI G., *Crime is Terribly Revealing: Information Technology and Police Productivity*, in *The Review of Economic Studies*, vol. LXXXVII, 2020, 11, 2732.

MATSAKIS Louise, *Scraping the Web Is a Powerful Tool. Clearview AI Abused It*, in *Wired*, 2020, *https://www.wired.com/story/clearview-ai-scraping-web[https://perma.cc/7VTF-KS66*].

MATTHEWS Richard, *How Law Enforcement Decodes Your Photos*, in *Conversation*, 2017, *http://theconversation.com/explainer-how-law-enforcement-decodes-your-photos-78828 [https://perma.cc/7RQ8-MX5C*].

MAYER Jonathan, MITCHELL John C., MUTCHLER Patrick, *Evaluating the Privacy Properties of Telephone Metadata*, in *PNAS*, 2016, 5536, 113.

MCCLURG AJ, "*In the Face of Danger: Facial Recognition and the Limits of Privacy Law*.", in *Harvard Law Review*, vol. CXX, no. 7, 2007, 1870 e 1891., *http://www.jstor.org/stable/40042639*;

MCFARLAND Matt, *Terrorist or Pedophile? This Start-Up Says It Can Out Secrets by Analyzing Faces*, in*WASH. POST*, 2016.

MCKINNEY Matt, *The Next Crime*, in *Star Trib*., Minneapolis, 2011, 1.

MENDELSON Aaron, *Can LAPD Anticipate Crime with Predictive Policing*?, in *Calif. Rep*., 2013, *http://audio.californiareport.org*.

MERLER MICHELE, RATHAN ALINI, FERIS ROGERIO & SMITH JOHN R., *Ibmrsch., diversity in faces*, 2019, 4, *https://arxiv.org/pdf/1901.10436.pdf, [https://perma.cc/ Z5BU-XXP9*]

MEROLA Linda &LUM Cynthia, *Emerging Surveillance Technologies: Privacy and the Case of License Plate Recognition* (*LPR) Technology*, in *JUDICATURE* 96:3 119-21, 2012.

MESSINETTI R., *Circolazione dei dati personali e autonomia privata*, in *Federalismi*, fasc. XXI, 2019, 5.

METZ, *California lawmakers ban facial-recognition software from police body cams*, in *www.edition.cnn.com*, 2019.

MITCHELL Robert L., *It's Criminal: Why Data Sharing Lags among Law Enforcement Agencies*, in *COMPUTER WORLD*, 2013, *www.computerworld.com.*

MITNICK Eric. J., *Procedural Due Process and Reputational Harm: Liberty as Self-Invention*, in *U.C. DAVIS*, 2009, 79-126, 43;

MOBILIO G., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative, Editoriale Scientifica*, Napoli, 2021, 32 ss, 57 ss, 240 ss.

MOHLERG.O. et al., *Randomized Controlled Field Trials of Predictive Policing*, in *J. Am. Stat. Assoc.*, 2015, 1399, 110.

MOHLERG.O. et al., *Self-Exciting Point Process Modeling of Crime,* in*J. Am. Stat,* 2011,Ass'n, 100, 106.

MORABITO C., *La chiave del crimine,* cit., 2015, 36 e 38.

MORRISON, *"Racist" facial recognition technology used in law enforcement, banking and schools misidentifies African American and Asian people 100 times more often than whites, study shows*, in *www.dailymail.co.uk*, 2019.

MOZUR Paul, *Chinese Man Caught by Facial Recognition at Pop Concert*, in *BBC News*, 2018, *https://www.bbc.com/news/world-asia-china-43751276[https://perma.cc/9DFT-5H3C];*

MOZUR Paul, *Inside China's Dystopian Dreams, A.I. Shame and Lots of Cameras*, K, 2018, *https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html [https://perma.cc/8J37-2NEK*]

MOZUR Paul, *One Month, 500,000 Face Scans: How China Is Using A.I. To Profile a Minority*, in *N.Y. Times*, 2019, *https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html*[*https://perma.cc/Z9QR-PG6F*].

MOZUR, *OneMonth, 500.000 Face Scans: How China Is Using A.I. to Profile a Minority*, in *www.nytimes.com*, 2019.

MOZUR e KROLIK, *A Surveillance Net Blankets China's Cities, Giving Police Vast Powers*, in *www.nytimes.com*, 2019,

MURATORE M.G., *La misurazione del fenomeno della criminalità attraverso le indagini di vittimizzazione*, 2011.

MURPHY Erin, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, in *CAL*2007, 721-728 ss, 795.

MYERS Laura, PARRISH Allen &WILLIAMS Alexis, *Big Data and the Fourth Amendment: Reducing Overreliance on the Objectivity of Predictive Policing*, in *CTS*, 2015, 231-234, 8.

MYRICK Amy, *Facing Your Criminal Record: Expungement and the Col- lateral Problem of Wrongfully Represented Self*, in *L. & SOC'Y*, 2013, 73, 47, 91.

NAKAR Sharon & GREENBAUM Dov, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, in *B.U.J. Sci. & Tech*, 2017, 88-94, 23

NEAGLE Colin, *How the Internet of Things Is Transforming Law Enforcement*, in *Network World*, 2014.

NISSAN E., *Digital Technologies and Artificial Intelligence's Present and Foreseeable Impact on Lawyering, Judging, Policing and Law Enforcement*, in *AI&Soc*., 2017, 450 ss., 31;

NIXON Ron, *U.S. Postal Service Logging All Mail for Law Enforcement*, in *N.Y.TIMES* , 2013.

NOBLE SAFIYAUMOJA, *Algorithms of oppression: how search engines reinforce racism*, 2018,

O'DONNEL R.M., *Challenging Racist Predictive Policing Algorithms under the Equal Protection Clause*, in *New York University Law Review*, 2019, 544 ss.

O'KEEFE David, *Head of the Manhattan District Attorney's Crime Strategies Unit*, in *CTR. FOR CT. INNOVATION*, 2013.

OHM Paul, *The Underwhelming Benefits of Big Data*, in *U. Pa.*, 2012, 339-340, 161, *https://www.pennlawreview.com/wp-content/uploads/2020/05/161-U-Pa -L-Rev-Online-339.pdf* [*https://perma.cc/U3FS-B9M8*]

O'NEIL CATHY, *Weapons of math destruction: how big data increases inequality and threatens democracy*, 2016, 98.

O'NEILL James, *Opinion, How Facial Recognition Makes You Safer*, in *N.Y. Times*, 2019, *https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [https://perma.cc/HDY6-FJ35]*.

ORWELL George, *Nineteen Eighty-Four*, Londra, 1949.

OSWALD M. – GRACE J. - URWIN S. – BARNESG.C., *Algorithmic risk assessment policing models: lessons from the Durham HART model and "Experimental" proportionality*, in *Information and Communications Technology Law*, 2018, 227.

PAPACHRISTOS Andrew V., Commentary: *CPD'S Crucial Choice: Treat Its List as Offenders or as Potential Victims*?, in *Chi. Trib.* , 2016;

PAPACHRISTOS Andrew, BRAGA Anthony A.,& HUREAU David M., *Social Networks and the Risk of Gunshot Injury*, in *J. Urb. Health*, 2012, 89,992.

PARODI Cesare e SELLAROLI Valentina, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo (DPC),* VI , 2019, 56, 59 e 61 ss.

PASQUALE FRANK, *The black box society 18,* 2015;

PATEL Faiza, LEVINSON-WALDMAN Rachel, DENUYL Sophia, and KOREH Raya, *Map: Social Media Monitoring by Police Departments, Cities, and Counties*, in *Brennan ctr. for just.*, 2019, *https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties, [https://perma.cc/ TC22-49A3*]

PATTERSON Thom, *Data Surveillance Centers: Crime Fighters or "Spy Machines*"?, in *CNN*, 2014, available at *www.cnn.com.*

PATTON, D.U. et al, *Stop and frisk online: theorizing every- day racism in digital policing in the use of social media for identification of criminal conduct and associations,* in *Social Media Society*, 2017, *https://doi.org/10.1177/20563 05117733344.*

PAUL Jeffrey S. & JOINER Thomas M., *Integration of Centralized Intelligence with Geographic Information Systems: A Countywide Initiative,* in *Geography &Pub. Safety*, 2011, 5 e 7.

PAULSEN Derek J. &ROBINSON Matthew B., *Crime mapping and spatial aspects of crime,*2d ed., 2009, 154.

PEARSALL Beth, *Predictive Policing: The Future of Law Enforcement*?, in N*at'l Inst. Just. J*., 2010, 16

PELLICCIA R., *Polizia predittiva: il futuro della prevenzione criminale*, in *www.cyberlaws.it*, 2019, 2.

PEREZ Gisela & COOK Hilary, *Google, YouTube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App that Helps Law Enforcement*, in *CBS News*, 2020, *https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial -recognition-app [https://perma.cc/UE64-UZBA*];

PERRY Walter L., MCINNIS Brian, PRICE Carter C., SMITH Susan C., HOLLYWOOD John S., P*redictive policing, The Role of Crime Forecasting in Law Enforcement Operations*, in *Rand Corporation*, Santa Monica, 2013, 1 ss.

PETRESCU Virgil, *Face Recognition as a Biometric Application,* in *J. Mechatronics & Robotics* 2019, 237-240, 3.

PITTS Wayne J., *From the Benches and Trenches: Dealing with Out- standing Warrants for Deceased Individuals: A Research Brief*, in *JUST. SYS. J.*, 2009, 219-220, 30.

POMERANTZ Jeffrey, *METADATA, The MIT Press*, Massachusetts, 2015, 3 e 13.

PORTER Jon, *Facebook and LinkedIn Are Latest to Demand Clearview Stop Scraping Images for Facial Recognition Tech*, in *Verge*, 2020, *https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter -youtube [https://perma.cc/AX4H-A9BJ]*.

PORTER, *Federal study of top facial recognition algorithms finds "empirical evidence" of bias*, in *www.theverge.com*, 2019;

POSTON Ben, *Crime in Los Angeles Rose in All Categories in 2015, LAPD Says,*in *L.A.times* , 2015.

POTTER Ned, Privacy Battles: *OnStar Says GM Can Record Car's Use, Even If You Cancel Service*, in *ABCNEWS* , 2011 *http://abcnews.go.com*.

PURI R., *Mitigating Bias* in *AI Models,* in *IBM*, 2018

PURSHOUSE J, CAMPBELL L, *Automated facial recognition and policing: A Bridge too far?, in Legal Studies*, 2022, 209. .

QUATTROCOLO S., *Intelligenza artificiale e giustizia: nella cornice della carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen.*, 2018.

QUINTARELLI S., *Intelligenza artificiale. Cos'è davvero, come funziona, che effetti avrà, Bollati Boringhieri,* (a cura di), *Milano, 2020;* CHIRIATTI M., *Incoscienza artificiale. Come fanno le macchine a prevedere per noi,* in *Luiss University Press, Roma,* 2021.

RAJAGOPALAN Megha, *Cellphone Companies Will Share Your Location Data—Just Not with You*, in *PROPUBLICA*, 2012, *www.propublica.org*.

RECCHIA N., *Il principio di proporzionalità nel diritto penale*, Torino, 2020, 252 ss.

REEL Monte, *Secret Cameras Record Baltimore's Every Move from Above*, in *Bloomberg business week*, 2016.

REICHERT Corinne, *Clearview AI Is Looking to Expand Globally, Report Says*, in *CNET*, 2020, *https://www.cnet.com/news/clearview-ai-reportedly-looking-to-expand-globally [https://perma .cc/4UXM-6SRH*]

RELLY Victoria, PETRESCU Virgil, *Face Recognition as a Biometric Application*, in *J. Mechatronics & Robotics*, 2019, 237-240 ss, 3.

REYES Juliana, *Philly Police Will Be First Big City Cops to Use Azavea's Crime Predicing Software, in Technically Media inc., 2013, http://technical.ly.*

RHEE Nissa, *Study Casts Doubt on Chicago Polices Secretive "Heat List"* in *Chi. Mag.*, 2016.

RHEE Nissa, *Can Police Big Data Stop Chicago's Spike in Crime*?, in C*hristian Sci. Monitor*, 2016.

RICH Michael L., *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, in *U. PA.*, 2016, 871-876, 164.

RIVERO Nicolás, *The Little-Known AI Firms Whose Facial Recognition Tech Led to a False Arrest*, in *Quartz*, 2020, *https://qz.com/1873731/the-unknown -firms-whose-facial-recognition-led-to-a-false-arrest [https://perma.cc/8MMN -H9V6*]

ROACH J., *Microsoft improves facial recognition technology to perform well across all skin tones, genders*, 2018, articolo apparso sul sito della *Società Microsoft*,

ROBINSON David, *Buyer Beware A tard Look at Police "Threat Scores"*, 2016, *www.equalfuture.us*.

RONSIN X., LAMPOS V., MAÎTREPIERRE V., *In-depth study on the use of AI in judicial systems, notably AI applications processing judicial decisions and data*, cit.

RONSIN X., LAMPOS V., MAÎTREPIERREA., *Questioni specifiche della giustizia penale: prevenzione del reato, del rischio di recidiva e valutazione del livello di pericolosità*, *Appendice I: Studio approfondito sull'utilizzo dell'intelligenza artificiale [IA] nei sistemi giudiziari, segnatamente delle applicazioni dell'intelligenza artificiale al trattamento di decisioni e dati giudiziari*, in *www.coe.int*, 35;

ROTH Andrea, *Safety in Numbers? Deciding When DNA Alone Is Enough to Convict*, in *N. Y.U.*, 2010, 1130-1134, 85.

RUBIN Joe, *Stopping Crime before It Starts*, in *L.A. Times*, 2010.

RUHA BENJAMIN, *Race after technology: abolitionist tools for the new jim code*, 2019, 112 s.

RUSHIN Stephen, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH.&POL'Y 281, 285-86.

SA'ADAH Rafael, *Acting Deputy Fire Chief, District of Columbia Fire and Emergency Medical Services Department*, 2015.

SA'ADAH Rafael, *Assistant Chief, District of Columbia Fire and Emergency Medical Services Department*, 2016.

SABELLI C., *Scacco alla malavita: arriva l'algoritmo che prevede i reati*, in *Il Messaggero*, 2017.

SACCHETTO E *New York City Bar, Power, Pervasiness and Potential: the Brave New World of Facial Recognition Through a Criminal Law Lens (and beyond)*, 2020, in *http://documents.nycbar.org.s3.amazonaws.com/files/2020662-BiometricsWhitePaper.pdf.*

SACCHETTO E., *Face to face*: il complesso rapporto tra *automated facial recognition technology* e processo penale, in *www.lalegislazionepenale.it*, 2020..

SAUNDERS Jennifer, HUNT Priscilla, & HOLLYWOOD John S., *Predictions Put into Practice: A Quasi-Experimental Evaluation of Chicago's Predictive Policing Pilot*, in J. *Experimental Criminol.*, 2016, 347-355-364, 12.

SCHLOSSBERGMARCH Tatiana, *New York Police Begin Using ShotSpotter System to Detect Gunshots*, in *N.Y. Times*, 2015.

SCHNEIER, *We're Banning Facial Recognition. We're Missing the Point*, in *www. nytimes.com*, 2020.

SCHUPPE Jon, *How Facial Recognition Became a Routine Policing Tool in America*, in *NBC News*, 2019, *https://www.nbcnews.com/news/us -news/how-facial-recognition-became-routine-policing-tool-america-n1004251[https://perma.cc/P3A4-KYJR*].

SCOVACRICCHI C., *Quando il poliziotto diventa startupper. La storia di* Keycrime, in *www.startupmagazine.it*, 2018.

SELBST Andrew D., *Disparate Impact in Big Data Policing*, in *GA.*, 2017, 109-113,52.

SELBST Andrew D. & BAROCAS Solon, *The Intuitive Appeal of Explainable Ma- chines*, in *Fordham* , 2018, 1085, 1090, 87 .

SELBST Andrew D., DANAH BOYD, FRIEDLE Sorelle A. r, VENKATA SUBRAMANIAN Suresh & VERTESI Janet, *Fairness and Abstraction in Sociotechnical Systems*, in *Conf. on fairness, accountability & transparency*, 2019, 59 *https://dl.acm.org/doi/ pdf/10.1145/3287560.3287598, [https://perma.cc/V79B-WULJ*];

SEYBOLD Steven D., Note, *Somebody's Watching Me: Civilian Oversight of Data-CollectionTechnologies*, in *TEX.*, 2015, 1029-1032, 93;

SHANE Peter M., *The Bureaucratic Due Process of Government Watch Lists*, in *GEO. WASH.*, 2007, 804-808, 75.

SHEEHAN Charles, *Sex Offenders Slip Away*, CHI. TRIB., 2006, *http://articles .chicagotribune.com/2006-03-31/news/0603310164_1_number-of-sex-offenders-parole-illinois-prisoner-review-board*;

SIMMONS Kami Chavis, ‘*’The Politics of Policing: Ensuring Stakeholder Collaboration in the Federal Reform of Local Law Enforcement Agencies*’’, in *J. CRIM. L. &CRIMINOL.*, 2008, 489-490, 98.

SIMONCINI A., *L’algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà,* in *BioLaw Journal*, 1/2019, 73 ss.

SIMONITE Tom, *Photo Algorithms ID White Men Fine—Black Women, Not So Much*, in *Wired*, 2018, *https://www.wired.com/story/ photo-algorithms-id-white-men-fineblack-women-not-so-much, [https://perma.cc/ M5CM-JNXR*].

SINGER e METZ, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, in *www.nytimes.com*, 2019.

SINGH J. P. et al., *A comparative study of violence risk assessment tools: a systematic review and meta-regression analysis of 8 studies involving 25980 participants, in Clin Psychol Rev*, 31, 2011, pp. 499 ss.

SKLANSKY David Alan, *the persistent pull of police professionalism*, 2011, 8 s., *http://www.hks.harvard.edu/var/ezpsite/storage/fckeditor/file/pdfs/centers-programs/programscriminal-justice/ExecSessionPolicing/NPIP-ThePersistentPullofPoliceProfessionalism-03-1l1.pdf*, 9.

SMITH Jack IV, *'MinorityReport' is Real-And It's Really ReportingMinorities, MIC,* 2015.

SMITH Laura M. et al, *Adaption of an Ecological Territorial Model to Street Gang Spatial Patterns in Los Angeles*, in *Discrete & continuous dynamical sys*., 2012,32, 3223.

SNOW Jacob, *Amazon’s Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, in *Aclu*, 2018, *https://www.aclu.org/blog/privacytechnology/surveillance-technologies/amazons-face-recognition-falsely-matched-28* [*https://perma.cc/9JS3-6TRM*].

SORO A., *La protezione dei dati personali nell’era digitale, in Nuova Giur. Civl*, 2019, 2, 343 ss.

SPIELMAN Fran, *ACLU Sounds the Alarm About Bill Allowing Use of Drones To Monitor Protesters*, in *Chi.sun-times*, 2018, 5:17 PM, *https://chicago.suntimes.com/politics/aclu-sounds-the-alarm-about-bill-allowing-use-of-drones-to-monitor-protesters[https:// perma.cc/T64R-SS94*].

STEINBOCK Daniel J., *Data Matching, Data Mining, and Due Process*, in *GA.*, 2005, 1-30, 40.

STRAHILEVITZ Lior Jacob, Reputation Nation: *Law in an Era of Ubiquitous Personal Information*, in *NW. U.*, 2008, 1667-1720, 102; R. SLOBOGIN Christopher, *Transactional Surveillance by the Government*, in *MISS*, 2005, 139-145, 75.

STROUD Matt, *The Minority Report, Chicago's New Police Computer Predicts Crimes, but Is It Racist*? In *Verge*, 2014, *www. theverge.com.*

STUART Tessa, *The Policemen's Secret Crystal Ball*, in S*antacruz Wkly*., 2012, 9, 13 s.

SUK Jeannie, *Criminal Law Comes Home*, in *YALE*, 2006, 2, 15-16, 116.

SULLIVAN Bob, *Who’s Buying Cell Phone Records Online? Cops,* in *MSNBC*, 2006, *www.msnbc.msn.com*;

SZPALLER Keila, *City of Missoula Makes Wrongful Arrests on Invalid Warrants*, in *Missoulian*, Missoula, 2013.

TALBERT Jeffery et al., *Pseudoephedrine Sales and Seizures of Clandestine Methamphetamine Laboratories in Kentucky*, in *JAMA*2012, 1524, 308; BARDIN Jon, *Kentucky Study Links Pseudoephedrine Sales, Meth Busts*, in *L.A. TIMES*, 2012.

TALBOT David, *L.A.Cops Embrace Crime Predicting Algorithm*, in *MitTech. Rev.*, 2012.

TALLONJENNIFER A. ET AL., *ctr. for court innovation, the intelligence- driven prosecution model: a case study in the new york county district attorney's office,*2016, 5 ss.

TAXMAN, FAYE, and SPINNER David L. "*The Jail Addiction Services (JAS) Project in Montgomery County, Maryland: Overview of Results From a 24-MonthFollowup Study*.", *Unpublished manuscript Department of Criminology and Criminal Justice, University of Maryland*, 1996.

TECH POLICY, *40 groups have called for a US moratorium on facial recognition technology*, in *Mit Technology Review*, 2020.

THOMAS Emily, *Why Oakland Police Turned Down Predictive Policing, Vice Motherboard*, 2016.

TORRES Ella, *Black Man Wrongfully Arrested Because of Incorrect Facial Recognition*, in *ABC News*, 2020, *https://abcnews.go.com/US/black-man-wrongfully-arrested-incorrect -facial-recognition/story?id=71425751, [https://perma.cc/JF9M-3C8E*];

TORRES Ella, *Black Man Wrongfully Arrested Because of Incorrect Facial Recognition*, in *ABC News*, 2020, *https://abcnews.go.com/US/black-man-wrongfully-arrested-incorrect-facial-recognition/story?id=71425751, [https://perma.cc/JF9M-3C8E*].

TOUSSAINT, *Indian police are using facial recognition to identify protesters in Delhi*, in *www.fastcompany.com*, 2019.

TURING A.M., *Computing machinery and intelligence*, in Mind, 1950, 433.

ULLAH Eisa Anis Ishrat & KHANUMM Akheela, *A Comparative Study of Facial Recognition Systems*, in *Int'l J. Advanced rsch. comput. sci.*, (special issue no. 2), 2018 ,114, 9.

UMMARINO A., *Una introduzione ai software per il crime mapping*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, 2013, 147-148, 7.

URWIN S., *Written evidence submitted by Sheena Urwin, Head of Criminal Justice, Durham Constabulary*, in *www.parliament.uk*, 2018.

VALENTINO- DEVRIES, *How the Police Use Facial Recognition, and Where It Falls Short*, in *www.nytimes.com*, 2020.

VALLI R.V.O., *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, in IL PENALISTA, *2019*.

VIGANÒ F., *La proporzionalità della pena. Profili di diritto penale e costituzionale*, Torino, 2021, 277 ss.

VINCENT, *Moscow rolls out live facial recognition system with an app to alert police*, in *www.theverge.com*, 2020.

VIOLA L., *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Foro amm.*, 2018, 1598 ss.

VIOLA L., voce *Giustizia predittiva*, in *"Diritto Online" Treccani,* 2018, CASTELLI C.– PIANA C., *Giustizia predittiva. La qualità della giustizia in due tempi*, in*questionegiustizia.it*; per un'analisi dell'esperienza francese GARAPON A., LASSÈGUE J., *Justice Digitale. Révolution graphique et rupture anthropologique*, Paris, 2018.

VIOLA L., voce *Giustizia predittiva*, in *"Diritto Online" Treccani,*2018,

VLADECK David C., *Consumer Protection in an Era of Big Data Analytics,* in *OHION.U.* 2016, 493-495, 42.

VUONG Zen, *Alhambra Police Chief Says Predictive Policing Has Been Successful*, in *Pasadena Star-News*, 2014.

WALKER Samuel, *The New Paradigm of Police Ac-countability: The U.S. Justice Department "Pattern or Practice" Suits in Context*, in *ST. LOUIS U. PUB.*, 2003, 3-8, 22.

WATTERS Ethan, *ShotSpotter*, in W*ired*, 2007, 146 e 152.

WEISBAUM Herb, *Big Data Knows You're Pregnant (and That's Not All)*, in *CNBC*, 2014, *www.cnbc.com*.

WEISE Karen, *Will a Camera on Every Cop Make Everyone Safer? Taser Thinks So*, in *Bloomberg business week*, 2016.

WHEELER Brian, *Police Surveillance: The US City That Beat Big Brother*, in *BBC NEWS MAG.*, 2016, *www.bbc.com.*

White House, Office of the Press Secretary, *Fact sheet: white house police data initiative highlights new commitments*, 2016.

WILLIAMS Robert, *Opinion, I Was Wrongfully Arrested Because of Facial Recognition. Why Are Police Allowed to Use It?*, in *Wash. post*, 2020, *https:// www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology, [https://perma.cc/XRD7-JFVR*]

WILSON Simone, *L.A. Sheriff's Creepy New Facial-Recognition Software Matches Surveillance Video with Mug Shot Database*, in *L.A. wkly.*, 2012.

WILTZ Teresa, *Facial Recognition Software Prompts Privacy, Racism Concerns in Cities and States*, in *Pew Statelin*, 2019, *https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/08/09/facial-recognition-software-prompts-privacy-racism-concerns-in-cities-and-states [https://perma.cc/4RJU -CV88]*.

WOHLSON Marcus, *Amazon's Next Big Business Is Selling You*, in *WIRED*, 2012.

WOODWARD John D., *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, in *U. Pitt.*, 1997, 97, 134, 59.

WRIGHT Joshua D., *The Constitutional Failure of Gang Databases*, in *STAN. J. C.R.&C.L.*, 2005, 115, 119-29, 2.

YUPERSIS S. & DIETRICHSHARON M., *nat'l consumer law ctr., broken records: how errors by criminal background checking companies harm workers and businesses,*2012, 7 e 20.

ZARA G., *Tra il probabile e il certo*, 2016, in *DPC—Diritto Penale Contemporaneo*, 12 ss.

ZARSKY Tal Z., *Governmental Data Mining and Its Alternatives*, in *PENNST.*, 2011, 285-287, 116

ZAUGG, *India is trying to build the world's biggest facial recognition system*, in *edition.cnn.com*, 2019,

ZHONG Ziyuan, *A Tutorial on Fairness in Machine Learning*, in *Medium*, 2018, *https://towardsdatascience.com/a-tutorial-on-fairness-in-machine-learning-3ff8ba1040cb*, *[https://perma.cc/HL42-9ZEJ*] .

ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, in RAFFAELLO CORTINA EDITORE (a cura di), Milano, 2015.

ZORLONI L., *Ho scoperto che la più discussa società di riconoscimento facciale al mondo ha le mie foto,* 2021, in *www.wired.it.*

ZUBOFF S., *The age of surveillance capitalism,*2019, 353 ss.