**Polizia predittiva e *smart city*: vecchie e nuove sfide per il diritto penale**

**di *Giulia Tavella***

SOMMARIO: 1. Introduzione. – 2. Polizia predittiva. – 3. Il quadro normativo attuale. – 4. Polizia predittiva e *smart city*. – 5. Vecchie e nuove sfide per il diritto penale.

## 1. Introduzione

Nel mondo si fa sempre più avanti l'idea della *smart city*, archetipo di città intelligente e interconnessa, capace di implementare soluzioni tecnologiche per i bisogni della società[1].

È stato osservato che la crescita del fenomeno *smart city* si ripercuote inevitabilmente sullo sviluppo della polizia predittiva e viceversa: se, da un lato, la città "intelligente" permette di incrementare i dati a disposizione dei *software* di polizia predittiva, dall'altro, questi ultimi ne condividono la strategia di efficienza, cercando di prevenire e/o contrastare la criminalità[2].

Invero, secondo un approccio di tipo prettamente economico, mentre fenomeni quali la raccolta della spazzatura o la gestione delle luci sono direttamente proporzionali all'efficienza della città, la criminalità, al contrario, ne è inversamente proporzionale, in quanto la sua presenza incide sull'economia del nucleo urbano. I *software* di polizia predittiva, pertanto, permetterebbero il raggiungimento di un "ottimo paretiano", consentendo di migliorare le *performance* investigative, nonché di allocare le risorse in maniera più efficiente.

Ciò sembra confermato anche da un recente studio, che ha dimostrato come l'utilizzo dei sistemi di polizia predittiva migliori la produttività delle forze dell'ordine in termini di repressione del crimine, mantenendo un ottimo rapporto costi-benefici. In particolare, l'autore ha esaminato la relazione empirica tra l'utilizzo del *software* Keycrime e la produttività dei pattugliamenti di polizia misurata dalla probabilità

[1] Sebbene non ci sia una definizione unanime del concetto di *smart city*, come tale generalmente si intende un'area urbana in cui le reti e i servizi tradizionali sono resi più efficienti attraverso l'uso di tecnologie digitali e di telecomunicazione, a beneficio degli abitanti e delle imprese. Ciò comporta, ad esempio, reti di trasporto urbano più intelligenti, forniture d'acqua migliorate e strutturate per lo smaltimento dei rifiuti, modi più efficienti per illuminare e riscaldare gli edifici, così come un'amministrazione cittadina più interattiva e spazi pubblici più sicuri. La definizione è ripresa dal sito https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en

[2] V. E.E. Joh, *Policing the smart city*, in *International Journal of Law in Context*, 15/2019.

che gli autori dei reati siano arrestati, utilizzando dati relativi a rapine a danno di esercizi commerciali e banche sul territorio di Milano lungo un arco temporale di due anni e mezzo[3].

Non sono mancate, tuttavia, voci discordanti, che non solo hanno ritenuto non dimostrata la maggiore capacità dei *software* predittivi di prevedere e contrastare i reati[4], ma ne hanno evidenziato anche il *vulnus* che da questi potrebbe derivare in termini di tutela dei cittadini e garanzia dei loro diritti[5].

Ad ogni modo, il contributo trasformativo delle nuove tecnologie sembra ormai innervare ogni campo dell'esistenza e costringe ad una costante riflessione anche sul piano giuridico, ove tante sono le sfide.

Il presente scritto, dopo una breve ricostruzione della pratica di polizia predittiva e del quadro normativo attuale in cui opera, evidenzia due aspetti derivanti dalla sua intersezione con il discorso organizzativo della *smart city*. Il primo profilo attiene all'ingente aumento di dati raccolto dai sensori sparsi sul territorio cittadino, i quali potranno essere successivamente impiegati dai sistemi di polizia predittiva che su questi si basano. Il secondo concerne la possibilità che l'attività di prevenzione venga incorporata nella stessa architettura urbana, con la conseguenza che più le città divengono *smart*, connesse vigili, più la polizia potrebbe diventare un aspetto meno visibile e più integrato dell'ambiente urbano. In entrambi i casi appare necessario vagliarne la compatibilità con i principi del diritto penale, mettendo in luce fin da subito che ciò potrebbe scalfirne – quantomeno in via potenziale – qualche certezza.

## 2. Polizia predittiva

Con l'espressione "polizia predittiva" (*predictive policing*) si intende l'utilizzo di tecniche analitiche, e in particolare quantitative, per identificare possibili *target* per l'intervento della polizia, prevenire la

[3] Cfr. G. Mastrobuoni, *Crime is Terribly Revealing: Information Technology and Police* Productivity, in *The Review of Economic Studies*, Vol. 87, Issue 6, 2020, 2727-2753. V. anche, L. Giraldi, *Intelligenza artificiale e* predictive policing *nella rinnovata fase di indagine*, in A. Massaro (a cura di), *Intelligenza artificiale e giustizia penale*, Paruzzo, 2020, 39-92, 48. Secondo l'autore, tale maggiore efficienza è dovuta principalmente al fatto che le risorse, anche se limitate, e i dati in possesso delle autorità vengono sfruttati in maniera ottimizzata rispetto al passato. Da un lato, infatti, un simile impiego delle risorse permette il raggiungimento, *mutatis mutandis*, di un "ottimo paretiano" investigativo; dall'altro, concede alla polizia giudiziaria, intesa in senso lato, di organizzare strategie operative e decisionali più efficienti

[4] V. S. Tulumello, F. Iapaolo, *Policing the future, disrupting urban policy today. Predictive policing, smart city and urban policy in Memphis (TN)*, in *Urban Geography*, 2019. Nell'articolo gli autori contestano l'effettiva capacità dei sistemi di polizia predittiva di prevenire i reati, svolgendo uno studio sul *software* Blue CRUSH (Crime Reduction Utilizing Statistical History), un programma di polizia predittiva sviluppato dal Dipartimento di Polizia di Memphis negli Stati Uniti d'America.

[5] Sul punto, *ex plurimis*, A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà,* in *BioLaw Journal,* 2019; G. Contissa, G. Lasagni, G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di internet*, 4/2019; V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020; F. Basile, *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, in *Dir. Pen. Uomo*, 2019.

commissione di reati futuri[6] e risolvere crimini passati facendo uso di metodi statistici sia nella fase di prevenzione[7] che investigativa[8]. Tale "previsione"[9] si basa sulla rielaborazione probabilistica di una serie di dati che riguardano sia la commissione di reati, sia i loro autori. Tra questi si annoverano i dati relativi a notizie di reati precedentemente commessi, agli spostamenti e alle attività di soggetti sospettati, ai luoghi teatro di ricorrenti azioni criminali e alle loro caratteristiche, al periodo dell'anno o alle condizioni atmosferiche maggiormente connesse alla commissione di determinati reati; talora, inoltre, vengono utilizzate anche informazioni circa l'origine etnica, il livello di scolarizzazione, le condizione economiche, le caratteristiche somatiche[10], riconducibili a soggetti appartenenti a determinate categorie criminologiche[11].

L'obiettivo di "predire" *chi* potrà commettere un reato, o *dove* e *quando* potrà essere commesso, pone necessariamente il fenomeno in una prospettiva *ante delictum*, limitata quindi alla fase antecedente l'esercizio dell'azione penale, in linea con l'approccio predittivo delle odierne alternative algoritmiche che compongono quello che taluni hanno rinominato "sistema oracolare *legal-tech*"[12].

---

[6] Secondo la tesi degli "ottimisti", gli scenari della giustizia algoritmica permetterebbero addirittura il superamento del diritto penale per raggiungimento dei propri scopi. Ciò in quanto, se gli algoritmi, come da più parti prefigurato, si rivelassero davvero in grado di predire con assoluta infallibilità – e dunque di prevenire – la commissione di determinati reati, gli strumenti del diritto penale perderebbero in radice la propria utilità. Tali entusiasmi, tuttavia, non possono essere condivisi: l'utilizzo degli algoritmi nel campo della giustizia penale deve essere esaminato ed analizzato con attenzione, specialmente in considerazione delle evidenti tensioni con i diritti fondamentali. Sul punto, cfr. V. Manes, *Intelligenza artificiale e giustizia penale*, in U. Ruffolo (a cura di), *XXVI Lezioni di diritto dell'Intelligenza Artificiale*, Giappichelli Editore, 2021, 281.

[7] La Polizia di prevenzione è definita dall'art. 1, co. 1, R.D. 18 giugno 1931, n. 773 (Testo unico delle leggi di pubblica sicurezza).

[8] Secondo Perry et al.: «*Predictive policing is the application of analytical techniques — particularly quantitative techniques — to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions […] Another term used to describe the use of analytic techniques to identify likely targets is forecasting. Although there is a difference between prediction and forecasting, for the purposes of this guide, we use them interchangeably*», W.L. Perry, B. McInnis, C.C. Price, S.C. Smith, J.S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation, 2013, xiii; v. anche M. Papa, *Future Crimes: intelligenza artificiale e rinnovamento del diritto penale,* in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini Giuridica, 2020; F. Basile, *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, cit.; G. Contissa, G. Lasagni, G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi e IA*, cit.; L. Giraldi, *Intelligenza artificiale e* predictive policing *nella rinnovata fase di indagine*, e L. Grossi, Software *predittivi e diritto penale*, in A. Massaro (a cura di), *Intelligenza artificiale e giustizia penale*, cit.

[9] Il verbo "predire" rappresenta la traduzione italiana più comune sia del termine inglese "*to forecast"* che di quello "*to predict"*, entrambi relativi al concetto di anticipazione del futuro. Tuttavia, c'è una differenza tra i due: mentre "*to forecast"* fa riferimento ad una previsione oggettiva, scientifica, riproducibile e libera da distorsioni ed errori individuali, "*to predict"* presenta un'accezione maggiormente soggettiva, prevalentemente intuitiva, non riproducibile e soggetta, invece, a distorsioni individuali. In linea con questa distinzione, benché nella lingua italiana non si riscontrino conseguenze pratiche, nella lingua inglese sarebbe più corretto utilizzare il verbo "*to forecast*" e non "*to predict*", e gli aggettivi a questo conseguenti. Nella comunità scientifica, tuttavia, è più diffuso il termine *predictive policing* (e non *forecast policing*). Sul punto, cfr. W.L. Perry et al., *Predictive Policing*, cit., 1.

[10] Con il rischio di un "Lombroso 2.0", secondo la felice espressione di A. Giannini, *Lombroso 2.0: On AI and Predictions of Dangerousness in Criminal Justice*, in *RIDP*, Vol. 29, Issue 1, 2021.

[11] F. Basile, *Intelligenza artificiale e diritto penale*, cit., 10.

[12] L'espressione è di V. Manes, *L'oracolo algoritmico e la giustizia penale,* cit., 553. Sul punto, v. anche G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, in *Arch. pen.*, 3/2019; F. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. Pen. Cont.*, 4/2020.

Il concetto di polizia predittiva si è sviluppato negli Stati Uniti alla fine del secolo scorso e trova il suo fondamento nelle teorie della criminologia ambientale, secondo le quali è possibile prevedere la commissione di un fatto criminoso in base alla considerazione che un individuo tenderà a commettere un delitto ogni qual volta che i benefici derivanti dal crimine siano altamente desiderabili e vi sia l'opportunità di commetterlo[13].

Invero, tale attività di analisi e mappatura delle attività criminali in un'area geograficamente determinata non è nuova. Da tempo, infatti, i fattori sociali, demografici, economici, ambientali, nonché quelli derivanti da precedenti penali, rappresentano indici rilevanti quantomeno ai fini dell'allocazione delle risorse di polizia. Ciò che appare oggi innovativo, invece, è la capacità di analizzare in tempi molto brevi un enorme quantitativo di dati grazie allo sviluppo esponenziale delle tecnologie e alla loro capillare diffusione, nonché di estrarre, mediante algoritmi di *data mining*, dei *pattern* prima invisibili[14]. La principale utilità della polizia predittiva, infatti, giace nella scoperta di similitudini e analogie ricavate a seguito dell'analisi e comparazione di variabili che si relazionano costantemente fra loro[15]. A ciò si aggiungono due ulteriori vantaggi in termini di efficienza: i *software* predittivi contribuiscono a una migliore gestione del *know how* delle forze dell'ordine in un'area geografica specifica, svincolandone la conservazione dalla presenza fisica e competenza dei singoli agenti, e migliorano le *performance* investigative in condizioni di limitate risorse umane, consentendo una allocazione più proficua delle stesse[16].

A seconda dello scopo per il quale sono utilizzati, i sistemi di polizia predittiva sono classificabili in due macrocategorie[17]:

---

[13] Più diffusamente: «questa opportunità [di commettere un reato] è legata alla presenza di una serie specifica di fattori, definiti dalle teorie razionali del crimine ed, in particolare, dalla "teoria delle attività di routine": la presenza di un autore motivato (*motivated offender*) e di obiettivi/bersagli che suscitino "interesse" nell'offender (*suitable targets*), nonché, contestualmente, l'assenza di quello che viene definito "guardiano capace" (*capable guardian*), cioè di una persona – o di un sistema, ad esempio una serie di telecamere – che sia in grado di impedire che il crimine venga portato a compimento, o che quantomeno ne disincentivi il tentativo di realizzazione», cfr. R. Pelliccia, *Polizia predittiva: il futuro della prevenzione criminale?*, in *www.cyberlaws.it*, 9 maggio 2019, il quale, a sua volta, fa riferimento a F.P. Williams, M.D. Mc Shane, *Devianza e criminalità*, Il Mulino, 2002.

[14] Per *data mining* si intende l'insieme di tecniche e metodologie che hanno per oggetto l'estrazione di informazioni da grandi quantità di dati, attraverso metodi automatici o semi-automatici, e l'utilizzo scientifico, aziendale, industriale o operativo delle stesse. In particolare, il *data mining* produce una nuova conoscenza, in quanto evidenzia correlazioni e regolarità non apparenti dai dati in sé dissociati. Queste informazioni possono tradursi in *pattern*, idonei all'applicazione, sul presupposto che dati riferiti al passato possono rivelare schemi di azioni utili circa attività future. Sul punto, C. Sarra, Business Intelligence *ed esigenze di tutela: criticità del c.d.* Data Mining, in P. Moro, C. Sarra (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, FrancoAngeli, 2017, 41 ss.; v. anche S.H. Liao, P.H. Chu, P.Y. Hsiao, *Data Mining Techniques and Applications – A decade review from 2000 to 2011*, in *Expert Systems and Applications*, 39, 2012.

[15] L. Giraldi, *Intelligenza artificiale e* predictive policing, cit., 48.

[16] G. Contissa et al., *Quando a decidere in materia penale sono (anche) algoritmi e IA*, cit., 621.

[17] La distinzione è ripresa da F. Basile, *Intelligenza artificiale*, cit., 11. Tale classificazione è stata proposta, in primo luogo, in W.L. Perry et al., *Predictive Policing,* cit., 19 ss.; v. anche L. Giraldi, *Intelligenza artificiale e* predictive policing, cit., 59 ss.

– sistemi volti ad individuare le c.d. "zone calde" (*hotspot*): luoghi che, secondo calcoli statistici, costituiscono il possibile scenario dell'eventuale futura commissione di determinati reati (*crime mapping*). Tali previsioni permettono di intensificare i controlli proprio su territori "ad alto rischio"[18]. Esempi di sistemi di questo tipo sono Risk Terrain Modeling (RTM), specializzato nella predizione di reati di spaccio di sostanze stupefacenti in individuate aree urbane[19], e PredPol, un *software* sviluppato dalla collaborazione tra il dipartimento di polizia di Los Angeles e la UCLA[20], entrambi diffusi negli Stati Uniti. In Italia, si rammenta X-LAW, sviluppato dalla Polizia di Napoli e utilizzato nel campo della prevenzione dei reati c.d. "predatori"[21].

– sistemi volti ad individuare gli autori di crimini seriali (*crime linking*). Tali previsioni permettono, attraverso un meccanismo di profilazione, di individuare l'autore di un precedente reato ovvero di prevedere dove e quando un determinato soggetto ne commetterà un altro[22]. I risultati forniti da questi

[18] Per un approfondimento delle diverse tecnologie mediante le quali svolgere l'analisi delle "zone calde", si rinvia a W.L. Perry et al., *Predictive Policing,* cit., 19 ss.; cfr. anche L. Giraldi, *Intelligenza artificiale e* predictive policing, cit., 59 ss.

[19]«I ricercatori hanno elaborato questo sistema sottoponendo all'algoritmo RTM dati inerenti ai fattori ambientali e spaziali più frequentemente connessi alla commissione dei reati suddetti: presenza di luminarie stradali scarse o non funzionanti, vicinanza di locali notturni, di fermate di mezzi pubblici, di stazioni ferroviarie, di snodi di strade ad alta percorribilità, di bancomat, di compro-oro, di parcheggi scambiatori, infine, di scuole. Ciò ha consentito di elaborare una vera e propria "mappatura" di alcune grandi aree metropolitane al fine di individuare le "zone calde" dove più elevato risulta il rischio di spaccio di sostanze stupefacenti, con conseguenti benefici in termini di programmazione e attuazione di interventi di prevenzione della delinquenza connessa allo spaccio», cfr. F. Basile, cit., 11, che, a sua volta, rinvia a J.M. Caplan, L.W. Kennedy, J.D. Barnum, E.L Piza, *Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis to Explore the Dynamics of Criminogenic Behavior Setting*, in *Journal of Contemporary Criminal Justice*, 33(2), 2017, 133 ss.; J.M. Caplan, L.W. Kennedy, *Risk Terrain Modeling: Crime Prediction and Risk Reduction***,** Univ. of California Press, 2016**;** L.W. Kennedy, J.M. Caplan, E.L. Piza, *Risk Clusters, Hotspots and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies*, in *Journal of Quantitative Criminology*, 2010, 339 ss**.** Per maggiori informazioni sul sistema, si visiti il sito https://www.riskterrainmodeling.com/.

[20] «*PredPol grew out of a research project between the Los Angeles Police Department and UCLA. The chief at the time, Bill Bratton, wanted to find a way to use COMPSTAT data for more than just historical purposes. The goal was to understand if this data could provide any forward-looking recommendations as to where and when additional crimes could occur. Being able to anticipate these crime locations and times could allow officers to pre-emptively deploy officers and help prevent these crimes. Working with mathematicians and behavioral scientists from UCLA and Santa Clara University, the team evaluated a wide variety of data types and behavioral and forecasting models. The models were further refined with crime analysts and officers from LAPD and the Santa Cruz (California) Police Department. They ultimately determined that the three most objective data points collected by police departments provided the most accurate input data for forecasting: 1. crime type; 2. crime location; 3. crime date and time*», cfr. https://www.predpol.com/.

[21] «X-Law è un trovato tecnologico e metodologico ideato e implementato per sperimentare, per la prima volta in Italia, l'applicazione della Polizia Predittiva per la Sicurezza Urbana, (…) si basa sulla possibilità di poter prevedere, con l'impiego d'Intelligenza Artificiale, scippi, rapine, furti, borseggi, truffe e altri delitti di tipo cosiddetto "predatorio" che normalmente avvengono nelle nostre bellissime città. Il trovato nel suo insieme consiste in un protocollo tecnico e metodologico configurato per generare e impiegare strategicamente allarmi Predittivi georeferenziati di possibili crimini, elaborati secondo un esclusivo modello previsionale di Machine Learning», cfr. https://www.xlaw.it/presentazione/.

[22] Questi *software* cercano di profilare il possibile autore della serie criminale attraverso la raccolta e l'incrocio di una gran mole di dati, provenienti da varie fonti (immagini riprese da una telecamera o informazioni relative a precedenti analoghi reati, etc.) e prevederne eventuali futuri reati. L'idea di fondo è che alcune forme di criminalità si manifestano in un arco temporale e in una zona geografica molto circoscritti (c.d. *near repeat crimes*, o reati a ripetizione ravvicinata). Ad esempio, la commissione di una rapina sembrerebbe essere associata ad un elevato rischio di commissione di una nuova rapina, da parte degli stessi autori e in una zona geografica assai prossima al luogo del primo delitto, entro le successive 48 ore e, sia pur con un tasso di rischio

*software* potrebbero, inoltre, essere usati anche per ricostruire la carriera criminale del soggetto profilato, ossia per imputargli non solo il reato in occasione del quale egli è stato individuato, ma anche quelli precedenti costituenti la serie criminale ricostruita grazie all'archiviazione e all'elaborazione dei dati. A tale categoria appartiene il *software* italiano Keycrime, impiegato in materia di rapine a danno di esercizi commerciali e banche[23]. Altri *software* parimenti ispirati all'idea di *crime linking* sono Precobs in Germania[24] e Harm Assessment Risk Tool (HART) in Inghilterra[25].

Da questa breve ricostruzione appare evidente come si stia diffondendo l'utilizzo degli algoritmi nell'ambito delle attività di polizia di prevenzione e come tale pratica sia destinata ad aumentare in futuro[26].

### 3. Il quadro normativo attuale

A lungo l'utilizzo degli strumenti di polizia predittiva, e più in generale dei sistemi di intelligenza artificiale[27], non è stato oggetto di specifica disciplina, demandando le condizioni e le modalità del loro

---

decrescente, fino a tutto il mese successivo. Cfr. F. Basile, *Intelligenza artificiale*, cit., 12. V. anche A.G. Ferguson, *Predictive Policing and Reasonable Suspicion*, in *Emory Law Journal*, Vol. 67, Issue 2, 2012.

[23] Il *software* Keycrime è utilizzato dal 2008 sul territorio del Comune di Milano e dal 2009 su tutta la provincia del capoluogo lombardo. Originariamente elaborato presso la Questura di Milano e poi divenuto di proprietà di un'azienda privata, Keycrime nasce per individuare gli autori seriali di rapine a danno di esercizi commerciali e banche sul presupposto che è stato dimostrato che il 70% delle rapine di questo tipo siano riconducibili a condotte seriali. Recentemente è stata iniziata una ulteriore sperimentazione anche per i furti in appartamento. L'algoritmo utilizza dati di *input* riguardanti prevalentemente le caratteristiche fisiche dell'autore (corporatura, colore di capelli, età, sesso, etnia, etc.) e le circostanze in cui si è esplicata la condotta criminosa (utilizzo di armi da fuoco, tipo di esercizio rapinato, metodo di fuga, veicolo, etc.). Questi dati, così come avviene nel corso delle indagini preliminari, vengono acquisiti dalla polizia giudiziaria in sede di sommarie informazioni testimoniali ovvero attraverso l'acquisizione di immagini e/o video degli impianti di sorveglianza. Ciò che cambia attiene alla fase successiva, poiché i dati vengono trasferiti nel *software* che procede alla loro elaborazione e li confronta con gli altri dati contenuti nei *dataset*. A fronte dei dati di *input*, il sistema fornisce quale *output*: il collegamento fra reati (il *crime link* appunto), individuando la serie ascrivibile al medesimo autore, e le previsioni sul suo prossimo reato, ossia su quando, dove e come questi dovrebbe commetterlo. Cfr. M. Venturi, KeyCrime – *La chiave del crimine*, in *PrimoPiano*, 12/2014, disponibile su www.onap-profiling.org; R. Pelliccia, *Polizia predittiva,* cit.; L. Grossi, Software *predittivi e diritto penale*, cit. 162-170; G. Mastrobuoni, *Crime is Terribly Revealing*, cit.; https://keycrime.com/. Sul punto v. anche C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Dir. Pen Cont.*, 6/2019, 56.

[24] K. Seidensticker, F. Bode, F. Stoffel, *Predictive Policing in Germany*, Projekt SKALA, 2018, disponibile all'indirizzo http://nbn-resolving.de/urn:nbn:de:bsz:352-2-14sbvox1ik0z06.

[25] La polizia del Durham, in collaborazione con l'Università di Cambridge, ha messo a punto il sistema HART con l'obiettivo di promuovere processi decisionali che permettano di realizzare interventi mirati a ridurre il rischio di recidiva. In realtà, più che al *genus* dei sistemi di polizia predittiva, sembrerebbe più corretto ricondurre il sistema HART ai c.d. *risk assessment toools,* ossia a quegli strumenti computazionali in grado di calcolare se un soggetto si sottrarrà al processo o commetterà ulteriori reati, che operano in una fase successiva rispetto a quella di prevenzione e indagine. D'altra parte, è inevitabile che queste categorie, dai confini ancora sfocati, possano talvolta sovrapporsi. Cfr. M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Dir. Pem. Cont.,* 2019, 10 ss.

[26] Basti pensare al crescente numero di agenzie che fanno uso di *software* predittivi quale ausilio alle attività di indagine, evidenziato da G. Mastrobuoni, *Crime is Terribly Revealing*, cit., 3.

[27] La proposta di Regolamento della Commissione europea indica con il termine "intelligenza artificiale" (IA) una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle

impiego, nonché la valutazione e la valorizzazione dei loro risultati, alla sola iniziativa degli operatori di polizia e alla prassi.

Un primo passo verso la regolamentazione si è registrato nel dicembre 2018 con l'adozione della Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti da parte della Commissione europea per l'efficacia della giustizia del Consiglio d'Europa (CEPEJ)[28]. Tale documento, esempio emblematico di *soft law*[29], cristallizza cinque principi che devono rappresentare la cornice imprescindibile di qualsiasi futura disciplina in materia: il rispetto dei diritti fondamentali (e in particolare del diritto di accesso alla giurisdizione e del diritto ad un processo equo), il principio di non discriminazione, il principio di qualità e sicurezza nell'analisi dei dati e delle decisioni giudiziarie (ossia l'utilizzo di fonti certificate e dati intangibili, attraverso modelli concepiti in modo multidisciplinare, in un ambiente tecnologico sicuro), il principio di trasparenza e imparzialità (declinato nelle forme di accessibilità, comprensibilità e verificabilità esterna dei processi computazionali), e l'inderogabile possibilità di controllo da parte dell'utente (il c.d. *under user control*).

Nell'aprile 2021, la Commissione Europea ha presentato la proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale[30]. Nella proposta non viene regolata l'intelligenza artificiale in quanto tale, ma il suo ingresso nel mercato, la messa in uso e l'utilizzo nell'ambito dell'Unione europea dei sistemi che contengono tale tecnologia (i c.d. SIA, Sistemi di Intelligenza Artificiale[31]), nel tentativo di mantenere quanta più neutralità nei confronti della tecnologia in discussione e per non rischiare una veloce obsolescenza definitoria[32]. La proposta classifica i SIA in base al rischio di impatto negativo sui diritti fondamentali: più il prodotto è suscettibile di mettere in pericolo tali diritti, più severe sono le misure adottate per eliminare o mitigarne l'impatto, fino a vietare determinati prodotti ritenuti incompatibili. In particolare, il Regolamento identifica: SIA proibiti (Titolo

attività industriali e sociali. Il documento è reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206.

[28] Per un commento "a prima lettura" della Carta etica, v. S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen.*, 18 dicembre 2018; v. anche M. Gialuz, *Quanto la giustizia penale incontra l'intelligenza artificiale*, cit., 12 ss.

[29] S. Quattrocolo, *Intelligenza artificiale e giustizia*, cit. 3.

[30] Il documento è reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206.

[31] «Per "sistema di intelligenza artificiale" (sistema di IA) si intende un *software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono», cfr. art. 3, n. 1, Regolamento.

[32] Per un'analisi dei profili di criticità emersi fin dalla bozza di Regolamento, v. A. Lavorgna, G. Stuffia, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale: un passo necessario, ma non sufficiente, nella giusta direzione*, in *Dir. Pen. Cont.*, 2/2021.

II), SIA ad alto rischio (Titolo III) e SIA che richiedono una specifica regolamentazione (Titolo IV); si ipotizza la possibilità di una ulteriore categoria di SIA residuali[33].

Nell'ambito della giustizia penale, la categoria prevalente sembra essere rappresentata dai SIA ad alto rischio, ossia non proibiti in quanto tali, ma soggetti a requisiti aggiuntivi (specificati nei Capitoli 2-6); tra questi, infatti, rientrano quelli utilizzati per l'identificazione biometrica e la categorizzazione di individui (escludendo i SIA inquadrati come "proibiti"[34]), nonché, più in generale, quelli utilizzati dalle forze di polizia e nell'amministrazione della giustizia.

Con riguardo al profilo della gestione e protezione dei dati necessari per l'utilizzo dei *software* in questione, deve, invece, farsi riferimento al *Data protection reform package*, costituito dal Regolamento 2016/679/UE (GDPR) e dalla Direttiva 2016/680/UE, che sostituiscono, rispettivamente, la Direttiva 95/46/CE e la Decisione quadro 2008/977/GAI[35]. In particolare, la Direttiva 2016/680/UE, che costituisce una *lex specialis* rispetto al Regolamento, mira a stabilire norme minime relative alla «protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzioni di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica»[36].

A livello nazionale, la Direttiva 2016/680/UE è stata attuata con D.lgs. 18 maggio 2018, n. 51[37], il cui art. 8, riprendendo l'art. 11 della Direttiva, stabilisce il divieto di decisioni basate unicamente su trattamenti automatizzati (il c.d. criterio di non esclusività del dato algoritmico)[38]. Ne consegue che

---

33 *Ibidem*, 92.

34 Tra i SIA proibiti, invece, rientrano i sistemi di identificazione biometrica "a tempo reale" da remoto in spazi pubblici per funzioni di polizia, se utilizzati ai fini di sorveglianza indiscriminata. La proposta, tuttavia, prevede varie eccezioni che sembrano ammetterne l'uso sulla base di una valutazione "caso per caso" e mediante il ricorso a criteri di proporzionalità (art. 5, nn. 2-4, Regolamento). Nei SIA considerati a rischio inaccettabile rientrano anche alcune casistiche del riconoscimento facciale, specialmente laddove sia un'autorità pubblica ad utilizzarle, salvo eccezioni (art. 5, n. 1d, Regolamento). Cfr. A. Lavorgna, G. Stuffia, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza*, cit., 92-93.

35 Sul punto, P. De Hert, V. Papakonstantinou, *The new Police and Criminal Justice Data Protection Directive. A first Analysis*, in *New Journal of European Criminal Law*, 1/2016, 7 ss.

36 Cfr. art. 1, par. 1, Direttiva.

37 «1. Il presente decreto attua nell'ordinamento interno le disposizioni della Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa 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, nonché alla libera circolazione di tali dati, e che abroga la decisione quadro 2008/977/GAI del Consiglio. 2. Il presente decreto si applica al trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche e al trattamento non automatizzato di dati personali delle persone fisiche contenuti in un archivio o ad esso destinati, svolti dalle 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. 3. Il presente decreto non si applica ai trattamenti di dati personali: a) effettuati nello svolgimento di attività concernenti la sicurezza nazionale o rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea e per tutte le attività che non rientrano nell'ambito di applicazione del diritto dell'Unione europea; b) effettuati da istituzioni, organi, uffici e agenzie dell'Unione europea», cfr. art. 1 d.lgs. n. 51/2018.

38 Sull'interpretazione dell'espressione "decisione basata unicamente su un trattamento automatizzato", v. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., 16, che, a sua volta, richiama J. Sajfert, T. Quintel, *Data Protection Directive (EU)*

l'impiego di *software* di polizia predittiva, laddove non limitati all'allocazione delle forze di polizia sul territorio ma utilizzati anche ai fini dell'individuazione della responsabilità penale, non potrà costituire l'unico elemento sul quale basare la decisione in sede di giudizio. In particolare, quando viene in gioco la libertà personale dell'imputato, l'art. 8 deve essere letto insieme agli artt. 5 e 6 CEDU e all'art. 6 CDFUE, con l'effetto che il tradizionale diritto di accesso al giudice deve oggi essere declinato nel diritto dell'interessato a che sul suo *status* si pronunci un giudice "in carne ed ossa"[39], il quale dovrà tenere conto anche di elementi di prova ulteriori rispetto all'*output* del *software* predittivo[40].

D'altronde, tale esito interpretativo poteva già desumersi dalla normativa esistente. *In primis*, l'art. 192, co. 2, c.p.p. stabilisce che l'esistenza di un fatto non può essere desunta da indizi a meno che questi siano gravi, precisi e concordanti, con la conseguenza che l'*output* del *software* si presenta come solo uno dei tanti elementi che possono fondare il giudizio di responsabilità. Inoltre, i risultati dell'attività predittiva devono essere assunti nel rispetto della disciplina codicistica e, pertanto, tenendo conto dei divieti di utilizzabilità stabiliti dall'art. 191 c.p.p. e dal divieto di perizia criminologica di cui all'art. 220, co. 2 c.p.p. Il tutto, infine, deve essere letto nella cornice dell'art. 533 c.p.p., che impone al giudicante la valutazione di condanna al di là di ogni ragionevole dubbio, la cui connotazione di ragionevolezza è difficilmente riconducibile all'interno di un algoritmo[41] e, pertanto, "calcolabile"[42].

### 4. Polizia predittiva e *smart city*

Come anticipato, condizione indispensabile per l'elaborazione di strategie efficienti e previsioni attendibili da parte dei *software* di polizia predittiva è la disponibilità di dati e, in particolare, di *big data*[43]; di

*2016/680 for police and criminal justice authorities*, in M. Cole, F. Bohem (a cura di*), GDPR Commentary*, Edward Elgar Publishing Ltd., 2018, 10 ss.

[39] V. G. Ubertis, *Intelligenza artificiale*, cit., 83, il quale, riprendendo una nozione elaborata nell'ambito del dibattito internazionale sviluppatosi in seno all'ONU sulle armi autonome, parla di: «controllo umano significativo».

[40] Quanto all'impiego in sede processuale di elementi di prova ottenuti mediante l'utilizzo di *software* di polizia predittiva e, più in generale, di dati generati automaticamente – attraverso algoritmi e modelli computazionali –, il cui vaglio di attendibilità si scontra con il tradizionale diritto probatorio, v. S. Quattrocolo, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 3/2020. V. anche, M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale,* cit., 17; C. Parodi et al., cit. 61 ss.; G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale,* in *Sistema penale*, 8 gennaio 2021.

[41] Come ben sintetizzato da Canzio: «la legge (art. 101, co. 2 Cost.) e la ragione (art. 111, co. 6 Cost.) costituiscono presidi della razionalità del giudicare e fonti di legittimazione della giurisdizione e dei giudici». Cfr. G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale*, cit. 2.

[42] Pe una riflessione in merito al tema del diritto "calcolabile", v., *ex plurimis*, N. Irti, *Per un dialogo sulla calcolabilità giuridica,* in *Riv. Dir. Proc.*, 2016; A. Carleo (a cura di), *Calcolabilità giuridica*, Il Mulino, 2017.

[43] Sull'utilizzo di *big data* da parte delle forze dell'ordine nell'utilizzo di tecniche di polizia predittiva, v. A. Bonfanti, Big data *e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *MediaLaws*, 3/2018.

questi, una parte ingente viene catturata mediante i c.d. sensori (telecamere, microfoni, sensori di quantità fisiche, etc.) distribuiti nelle città[44].

La trasformazione dei centri urbani in *smart city* determina un incremento di sensori sul territorio cittadino, secondo la nota dinamica del c.d. *Internet of Things*[45], e, conseguentemente, un aumento della raccolta di dati che possono essere successivamente – ma anche *real-time*[46] – impiegati dai *software* predittivi[47].

In altre parole, tecnologie disegnate per raccogliere e manipolare dati al fine di migliorare l'efficienza della gestione di una città potranno essere sfruttate anche per le attività di polizia predittiva[48]. Ad esempio, un semaforo dotato di sensori per cui all'avvicinarsi di una macchina e in assenza di altri veicoli in attraversamento faccia scattare il verde permette la costante sorveglianza di quella specifica strada; ancora, un cestino che si auto-monitora per segnalare ai servizi di igiene urbana quando deve essere svuotato potrebbe allo stesso tempo raccogliere informazioni circa la tipologia di rifiuti e la frequenza con cui vengono gettati.

Non solo. La trasformazione in *smart city* potrebbe determinare un'ulteriore conseguenza, ossia che l'attività di prevenzione venga incorporata nella stessa architettura urbana[49]. Ciò significa non solo che strade, marciapiedi, palazzi, veicoli conterranno sensori capaci di raccogliere dati, ma che questi potrebbero anche essere capaci di fornire una immediata risposta automatica a comportamenti indesiderati. Ad esempio, si potrebbe precludere l'accesso a determinati luoghi a coloro che vengono identificati mediante un meccanismo di riconoscimento facciale come autori di precedenti reati; oppure un veicolo, interagendo con i sensori stradali, potrebbe impedire al guidatore di superare il limite di velocità consentito, di passare con il rosso, o, più in generale, di trasgredire una norma del Codice della

---

[44] I dati catturati dai sensori sono solo una parte del *dataset* a disposizione dei *software* di polizia predittiva. Si pensi alla mole enorme di dati ottenuti dal *social media mining*, ossia mediante l'estrazione di enormi quantità di dati grezzi sui *social network* per identificare tendenze comportamentali. Per uno studio circa l'utilizzo di Twitter al fine della predizione di reati, v. M. S. Gerber, *Predicting crime using Twitter and kernel density estimation*, in *Decision Support Systems*, Vol. 61, 2014.

[45] Sul punto, v. N. Climer, *Il cloud e l'Internet delle cose*, in J. Al-Khalili (a cura di), *Il futuro che verrà*, Bollati Boringhieri, 2017.

[46] Per esempio, la città di Natal (Brasile) ha aderito alla *IEEE Smart City Initiative* con l'obiettivo di trasformarsi in una *smart city* attraverso lo sviluppo di sistemi e applicativi per rinforzare l'uso delle tecnologie e migliorare la qualità della vita dei cittadini. All'interno di questa iniziativa è stata sviluppata ROTA, una piattaforma volta a migliorare la sicurezza pubblica mediante la raccolta, l'integrazione, l'analisi e la condivisione di informazioni riguardanti gli eventi che si verificano e i veicoli delle pattuglie di polizia. In particolare, i suoi due moduli (ROTA-PSM e ROTA PVM) sono applicazioni mobili utilizzate per monitorare la posizione delle pattuglie sul territorio e per supportarle nelle loro operazioni in tempo reale. V. A. Araujo, N. Cacho, A.C. Thome, A. Medeiros, J. Borges, *A Predictive Policing Application to Support Patrol Planning in Smart Cities,* 2017 International Smart Cities Conference (ISC2), IEEE, 2017.

[47] E.E. Joh, *Policing the smart city*, cit., 178 ss.

[48] *Ibidem*, 180. L'autrice definisce le funzionalità delle *smart cities* come "*dual-use technologies*".

[49] *Ibidem*. Secondo l'autrice, il *policing* è "inerente" alla *smart city*: man mano che le città divengono più *smart*, l'attività di *policing* è sempre più incorporata nell'infrastruttura urbana.

strada[50]. Tornando agli esempi precedenti, il semaforo dotato di sensori potrebbe interagire direttamente con il veicolo impedendo la trasgressione, mentre il cestino che si auto-monitora potrebbe allertare autonomamente le forze dell'ordine laddove rilevi un pacco sospetto.

Quindi, più le città divengono *smart*, connesse vigili, più la polizia potrebbe risultare meno visibile e più integrata nell'ambiente urbano.

Appare, pertanto, evidente la stretta sinergia esistente tra *smart city* e polizia predittiva, la cui genealogia parte da un presupposto comune: il tentativo di rendere la città oggetto del pensiero razionale, del calcolo di dati e del controllo[51]. Entrambe le dimensioni, infatti, condividono il focus sull'anticipazione e sulla gestione del futuro quale soluzione per risolvere i problemi presenti, e la concettualizzazione del problema urbano come una questione di soluzioni tecnologiche e tecnocratiche[52].

## 5. Vecchie e nuove sfide per il diritto penale

Rinviando ad altra sede l'analisi delle molteplici perplessità circa l'attendibilità dei sistemi di polizia predittiva[53] e le preoccupazioni da questi sollecitate con riguardo alle garanzie fondamentali e alla tutela dei principi costituzionali[54], vogliono qui evidenziarsi due ricadute critiche del binomio *smart city*/polizia predittiva sulla materia penale.

---

[50] Per un approfondimento in materia di *self-driving cars*, si rimanda al contributo di A. Cappellini, *Profili penalistici delle* self-driving cars, in *Dir. Pen. Cont.*, 2/2019.

[51] S. Mattern, *Mission control: A history of the urban dashboard*, in *Places Journal*, 2015.

[52] V. S. Tulumello, F. Iapaolo, *Policing the future, disrupting urban policy today*, cit.

[53] In particolare, si rammenta il rischio del c.d. *confirmation feedback loop*, ossia il rischio di innescare circoli viziosi. I *software* predittivi sono sistemi che si auto-alimentano con i dati prodotti dal loro stesso utilizzo: ad esempio, se un sistema individua un determinato *hotspot*, aumenteranno i controlli della polizia, con la conseguenza che aumenterà il tasso dei reati rilevati in quella zona, che diventerà, a sua volta, ancora più "calda". Le zone non considerate "calde", invece, in ragione del minor dispiego di forze dell'ordine, rischiano di rimanere, o di diventare, zone franche per la commissione di reati. Il problema si lega indissolubilmente con la tendenza degli algoritmi ad essere discriminatori. Infatti, sebbene le nuove tecnologie mettano a disposizione dell'investigatore un ampio patrimonio informativo disponibile per orientare l'attività operativa in maniera selettiva e proficua, allo stesso tempo possono essere basati su pregiudizi, che, a loro volta, tendono ad auto-avverarsi: se si vigila con più attenzione su determinate categorie, si scovano per ciò stesso più reati, anche se il tasso di criminalità non è realmente superiore alla media. Cfr. F. Basile, *Intelligenza artificiale e diritto penale*, cit., 13; P. Sorbello, *Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto*, in *Dir. pen. cont.*, 2/2019, 386; F. Ubertis, *Intelligenza artificiale*, cit., 10-11; V. anche K. Lum, W. Isaac, *To Predict and Serve?,* disponibile all'indirizzo **https://doi.org/10.1111/j.1740-9713.2016.00960.x**; A.G. Ferguson, *Predictive Policing and Reasonable Suspicion*, cit., 322..

[54] Le critiche avanzate nei confronti degli strumenti di polizia predittiva sono molteplici. *In primis*, tali *software* sollevano delle perplessità circa il rispetto del principio di uguaglianza (art. 3 Cost.); come ben sintetizzato da Manes: «l'algoritmo – per antonomasia – è anti-egualitario, perché considera alcuni fattori di rischio e non altri (età, genere, ma anche luogo di residenza, back-ground socioeconomico, abitudini di vita, tendenze sessuali o "morali", data di commissione del primo precedente, etc.), e su queste basi non solo suggerisce l'allocazione di maggiori risorse di polizia in alcuni contesti urbani piuttosto che in altri, ma pone una presunzione di maggior pericolosità in relazione ad alcuni soggetti e non ad altri», cfr. V. Manes, *L'oracolo algoritmico*, cit., 559. In secondo luogo, si pone il problema della tutela dei dati e del diritto alla *privacy*; sul punto, v. M.F. De Tullio, *La privacy e i* big data *verso una dimensione costituzionale collettiva*, in *Pol. dir.*, 2016, 662. Infine, non si deve trascurare la circostanza che la maggior parte di questi *software* sono coperti da brevetti depositati da aziende private, i cui detentori tendono

La prima attiene alla compatibilità di tale ricostruzione con i principi di materialità e di offensività, nonché con la finalità rieducativa della pena, e concerne i sistemi di polizia predittiva in generale, il cui utilizzo – come precedentemente evidenziato – è incrementato dall'ingente quantitativo di dati raccolti dai sensori delle *smart city*.

Nel racconto di Philip Dick "The Minority Report" la prevenzione del reato si spinge a punire un fatto non ancora commesso, ma che è stato preveduto da tre soggetti con sviluppate capacità cognitive impiegati a tale scopo da un immaginario dipartimento di polizia; per tale giustizia predittiva, infatti, anche la mera intenzione costituisce reato e determina delle conseguenze in punto di sanzione.

Questo scenario distopico non sembra realizzabile in un diritto penale liberale a base oggettivistica che richiede, ai fini della pena, la commissione di un fatto materiale di reato – così come sancito dall'art. 25, co. 2, Cost. – che, a sua volta, si sostanzi nell'effettiva offesa di un bene giuridico[55].

Sotto questo profilo, la prima categoria di sistemi predittivi, ossia quelli volti ad individuare i c.d. *hotspot*, non pongono particolari problemi, in quanto il loro utilizzo è circoscritto alla fase di allocazione delle risorse di polizia o, al più, all'individuazione di particolari zone dove potrebbe essere commesso un reato. In questo caso, la polizia si reca nel luogo indicato ed eventualmente impedisce la commissione di un reato o la "limita" alla forma del tentativo. Ne consegue che in sede giudiziaria, ancorando il giudizio di responsabilità al fatto commesso dall'agente, questo verrà punito per il solo tentativo di reato, salva l'applicazione di ulteriori provvedimenti da parte della polizia di prevenzione.

Lo stesso non può dirsi con riferimento ai sistemi di *crime linking*, che hanno lo scopo di individuare l'autore di un precedente reato ovvero di prevedere dove e quando un determinato soggetto ne commetterà un altro. In questo caso, si assiste ad uno spostamento del baricentro dall'accertamento del fatto di reato ad una verifica avente ad oggetto esclusivamente, o comunque eminentemente, il suo autore.

Riprendendo le considerazioni svolte altrove in tema di *risk assessment tools*[56], ciò rischia di determinare un passaggio dal "diritto penale del fatto" ad un "diritto penale d'autore" (o "del tipo criminologico dell'autore"), posto che il giudizio di responsabilità andrebbe a fondarsi non sul parametro oggettivo del fatto di reato commesso dall'agente, bensì su una valutazione della sua personalità[57]. Peraltro, tale

a non disvelare i propri segreti industriali e commerciali. Ciò determina una maggior difficoltà nella comprensione dei meccanismi del loro funzionamento, con evidente pregiudizio delle esigenze di trasparenza e di verifica della qualità e affidabilità dei risultati da essi prodotti, v. E.E. Joh, *Policing the smart* city, cit., 179-180.

[55] F. Mantovani, *Diritto penale. Parte generale*, 11a ed., Cedam, 2020. Si rammentano anche le voci autorevoli di N. Mazzacuva, *Il disvalore di evento nel diritto penale*, Giuffrè, 1983; F. Palazzo, *La recente legislazione penale*, Cedam, 1985; F. Sgubbi, *Il reato come rischio sociale. Ricerche sulle scelte di allocazione dell'illegalità penale*, Il Mulino, 1990.

[56] M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale,* cit., 19 ss.

[57] Come è noto, la formula "diritto penale d'autore" evoca la circostanza per cui non si punisce più il reato, ma il reo e, nello specifico, per "quello che è" non per "quello che fa", in contrasto con un sistema improntato sul diritto penale del fatto e

valutazione si fonderebbe su statistiche, schemi comportamentali generali e decisioni riferite a determinati gruppi di individui, ossia su un *tipo* di individuo e non sul *singolo* che riceverà la punizione, in evidente tensione con il principio di individualizzazione del trattamento sanzionatorio, e conseguentemente con la funzione rieducativa della pena garantita dall'art. 27, co. 1 e 3, Cost.

Se, dunque, il principio di materialità appresta un limite insuperabile alla responsabilità penale e la finalità rieducativa non consente di strumentalizzare l'individuo per fini generali di politica criminale, l'utilizzo di tale secondo gruppo di strumenti predittivi non è facilmente conciliabile con l'idea di giustizia penale. La trasformazione del centro urbano in *smart city*, sebbene non introduca un nuovo problema, ne consolida uno già esistente.

Il secondo profilo di interesse – per certi versi più innovativo – si presenta quale diretta conseguenza della considerazione secondo cui l'avvento delle *smart city* potrebbe determinare l'incorporazione dell'attività di prevenzione dei reati direttamente nell'architettura urbana[58].

Ciò potrebbe comportare due conseguenze. La prima è che, così facendo, l'algoritmo vada ad affiancare ed integrare la legge anche in materia penale[59], secondo la nota formula "*code is law*", per cui il diritto e la sua applicazione sono sostituite – se non *in toto,* almeno in larga parte – da una corrispondente infrastruttura informatica[60]. Invero, la disciplina dei fenomeni attinenti al sistema penale si avvia a essere

della colpevolezza. La letteratura sul tema è vasta; *ex plurimis*, L. Ferrajoli, *Il diritto penale del nemico e la dissoluzione del diritto penale*, in *Questione Giustizia*, 2006; M. Donini, M. Papa (a cura di), *Diritto penale del nemico. Un dibattito internazionale*, Giuffrè, 2007; F. Palazzo, *Contrasto al terrorismo, diritto penale del nemico e diritti fondamentali*, in *Questione giustizia*, 2/2006. Quanto alla declinazione del "diritto penale d'autore" con riferimento al formante algoritmico, cfr. G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, cit., 10.; V. Manes, *L'oracolo algoritmico e la giustizia penale,* cit., p. 559.

[58] La centralità dell'architettura nel fenomeno della regolamentazione è evidenziata anche da Lessig, il quale considera nel modello pre-Internet quattro diversi vincoli ai comportamenti degli individui: la legge, il mercato, le norme sociali e – appunto – l'architettura. Come primo vincolo l'individuo trova innanzitutto la legge, che prevede diritti, obblighi e sanzioni nel caso di inosservanza delle regole imposte. In secondo luogo, l'individuo è vincolato dalle norme sociali che influiscono sul modo di comportarsi, condannando colui che violi una regola ad una pena inflitta non dallo Stato, ma dalla comunità. Il terzo tipo di vincolo è costituito dalle leggi del mercato. Infine, l'ultimo vincolo è rappresentato dall'architettura, cioè dal mondo fisico e dalle condizioni simultanee dettate dall'ambiente naturale, che possono influire sul comportamento individuale, ma questa, diversamente dalle leggi e dalle norme sociali, non vincola attraverso sanzioni *ex post.* Cfr. L. Lessig, *Code and Other Laws of Cyberspace*, Basic books, 1999; v. anche E. Maestri, Lex informatica *e diritto. Pratiche sociali, sovranità e fonti nel* cyberspazio, in *Il Mulino Riv. web*, n. 1/2017.

[59] Nel settore civile, tale fenomeno sembra già in atto. Si fa riferimento ai c.d. *smart contract*; protocolli informatici basati sulla tecnologia *blockchain* che eseguono in modo automatico o semi-automatico i comandi stabiliti in sede di programmazione corrispondenti alle clausole negoziali stabilite dalle parti durante la contrattazione. Sul punto, v. S. Hassan, P. De Filippi, *The expansion of algorithmic governance: From code is law to law is code*, in *Field Actions Science Report*, Special Issue, 17, 2017. Per una efficace sintesi della letteratura sul tema, v. V. Dwivedi, V. Pattanaik, V. Deval, A. Dixit, A. Norta, D. Draheim, *Legally Enforceable Smart-Contract Languages: A Systematic Literature Review*, in *ACM Computing Surveys*, Vol. 54, n. 5, 2020.

[60] Con il sintagma "*code is law"* si indica l'idea che con l'avvento delle nuove tecnologie il codice informatico possa arrivare a regolare il comportamento di coloro che le utilizzano. Cfr. L. Lessig, *Code is law. On Liberty in cyberspace,* in *Harvard Magazine*, 2000, e già prima *Code and Other Laws of Cyberspace*, cit.; v. anche S. Hassan et al., *The expansion of algorithmic governance*, cit. Secondo alcuni autori, l'informatica e la digitalizzazione del diritto modificano non soltanto i mezzi di diffusione della legge, ma, più profondamente, la sua stessa elaborazione e il rapporto con il mondo. La scrittura numerica si inserisce nella produzione della norma e la giustizia predittiva (o giustizia digitale) va intesa come una fonte alternativa di normatività giuridica. Cfr. A.

regolata tramite codici algoritmici al punto che il primato delle norme incriminatrici disposte dalla legge viene sostituito dalle norme che regolano l'applicazione del *software*[61], con evidenti ricadute sul principio di legalità e sui corollari del nostro diritto penale "tradizionale"[62].

In secondo luogo, si apre la prospettiva di uno spostamento del paradigma penalistico dalla logica della sanzione alla logica della prevenzione e della *compliance*[63], generando «il progressivo appannamento della distinzione fra prevenzione e accertamento dei reati»[64]. In altre parole, se fino ad ora il diritto penale ha garantito la tutela dei beni giuridici in modo normativo e controfattuale, dunque intervenendo solo una volta commesso il fatto di reato, i sistemi di polizia predittiva – e di intelligenza artificiale in generale –, specie se incorporati nell'infrastruttura urbana, perseguono nel lungo periodo l'obiettivo della pratica impossibilità o almeno della sostanziale minimizzazione delle lesioni ai beni giuridici[65].

Tuttavia, una tale impostazione richiede anche una consapevole scelta politico-criminale, in quanto la costante sorveglianza nei confronti dei cittadini derivante dall'incorporazione della prevenzione nell'architettura urbana, che rende i fatti di reato *eo ipso* o *de facto* impossibili,[66] ne comprime

---

Garapon, J. Lasségue, *Justice digitale. Révolution graphique et rupture anthropologique*, PUF, Paris, 2018; E. Fronza, "*Code is Law". Note a margine del volume di Antoine Garapon e Jean Lasségue, Justice digitale. Révolution graphique et rupture anthropologique, PUF, Paris, 2018*, in *Dir. Pen. Cont.*, 11 dicembre 2018. Hildebrandt parla di "*technological normativity*" in contrapposizione alla "*legal normativity*", cfr. M. Hildebrandt, *Legal and technological normativity: more (and less) than twin sisters*, in *Technè: Research in Philosophy and Technology*, 12/2008; v. anche, M. Hildebrandt, *Code driven law. Freezing the future and scaling the past*, in C. Markou, S. Deakin (a cura di), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence*, Bloomsbury Publishing, 2020.

[61] «L'algoritmo tende a sostituire la legge. Al punto che il primato delle norme incriminatrici disposte dalla legge viene sostituito dalle norme che regolano l'applicazione del *software*: e ciò potrebbe accadere sia nel giudizio di fatto attinente alla individuazione di innocenza e colpevolezza dell'imputato, sia nel giudizio di diritto circa la definizione del confine tra lecito e illecito. Dunque, il testo della fattispecie incriminatrice diventa soltanto uno degli elementi che entrano nella piattaforma digitale per la gestione della *governance* giudiziaria», cfr. F. Sgubbi, *Il diritto penale totale*, Il Mulino, 2019, 41 ss.

[62] È, tuttavia, innegabile che il nostro diritto penale "tradizionale", e in particolare il suo principale strumento concettuale ossia la fattispecie incriminatrice, stia conoscendo un momento di forte crisi poiché è in crisi la possibilità di ordinare il mondo in base all'aspetto delle cose. Dinnanzi a tale crisi, si tratta di capire quale possa essere il possibile contributo delle nuove tecnologie, ossia se possiamo immaginare che queste ci conducano a un rinnovamento della fattispecie incriminatrice, a concepirne e svilupparne una nuova tipologia, che presenti nuove modalità di descrivere, comunicare il precetto penale. Cfr. M. Papa, *Future crimes*, cit., 4. Più diffusamente, M. Papa, *Fantastic voyage. Attraverso la specialità del diritto penale*, 2a ed., Giappichelli Editore, 2019; M. Papa, *La fattispecie come sceneggiatura dell'ingiusto: ascesa e crisi del diritto penale cinematografico*, in *Criminalia*, vol. 2019.

[63] Cfr. C. Bouchard, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. Ita. Dir. e Proc. Pen.*, 4/2019; secondo l'autore, l'intelligenza artificiale a è un costrutto sociale la cui prassi è in grado di trasformare le nostre basilari concezioni di ordinamento sociale e giuridico fino a decretare la fine del diritto penale per come noi lo conosciamo.

[64] G. Illuminati, *Editoriale*, in *Rev. italo-española der. proc.*, 1/2019, 1.

[65] Con evidenti ripercussioni sulle funzioni della fattispecie incriminatrice e, in particolare, della funzione comando. La fattispecie, infatti, è capace di orientare il comportamento dei cittadini ancora prima, e a prescindere, dalla minaccia della pena; cfr. M. Papa, *Fantastic voyage*, cit. 108 ss. V. anche C. Bouchard, *L'intelligenza artificiale come fine del diritto penale?*, cit., 1934.

[66] Secondo Brennan-Marquez, il *policing* produce "*a social order – a surveillance society – in which people constantly monitor and curate the data-trails they leave behind in everyday life*", cfr. K. Brennan-Marquez, *Big Data Policing and the Redistribution of Anxiety*, in *Ohio State Journal of Criminal Law,* 2018, 487. «L'ambizione della *legaltech* è diventare essa stessa la giustizia, tramite una rivoluzione numerica che rende mondi eterogenei compatibili fra loro, mettendo in comunicazione il diritto e la realtà mutevole del fatto. Il sogno segreto è di un mondo dove i rapporti sociali non saranno più gestiti dalla politica e dal diritto, bensì dalla tecnica, partendo dalla consapevolezza che l'opinione pubblica è più rassicurata da una decisione tecnica, che da una decisione umana, pur se presa nel rispetto di tutte le garanzie. La giustizia fatta dagli uomini rischia di venire considerata

indefettibilmente la libertà di "determinarsi altrimenti", con il rischio di una rottura con il tradizionale diritto penale liberale e una deriva verso forme di c.d. "paternalismo tecnologico"[67].

Le conseguenze prospettate, per la rilevanza e incidenza sui principi e sulle fondamenta stesse del nostro diritto penale, meritano un'adeguata attenzione nel discorso *smart city*/polizia predittiva, in quanto, a fronte degli innegabili vantaggi in termini di efficienza e di prevenzione e/o repressione del crimine, potrebbero verificarsi anche imprevisti e indesiderati cambi di paradigma.

arbitraria, fallace, un dato storico superato. Si è così messo in moto, dunque, un processo di *desimbolizzazione* della fragile umanità del diritto e del giudice e una *resimbolizzazione* in termini scientifici», cfr. E. Fronza, "*Code is Law". Note a margine del volume di Antoine Garapon e Jean Lassègue, Justice digitale,* cit.

[67] Tanto più si producono previsioni comportamentali volte alla prevenzione del crimine basate sul diffuso impiego di dati, tanto più è favorita l'internalizzazione da parte dei singoli soggetti del progetto stesso di prevenzione del crimine. L'individuo, infatti, impegnandosi nel progetto tecnologico-informatico di inibizione del crimine attraverso il monitoraggio del rischio altrui, lo fa a costo di monitorare se stesso, accetta tutto questo come proprio e diventa così l'esecutore delle strutture di potere alla base di questo progetto di sorveglianza, cfr. C. Bouchard, *L'intelligenza artificiale come fine del diritto penale?*, cit., 1937.

**Bibliografia**


Araujo A., Cacho N., Thome A.C., Medeiros A., Borges J., *A Predictive Policing Application to Support Patrol Planning in Smart Cities,* 2017 International Smart Cities Conference (ISC2), IEEE, 2017

Basile F., *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, in *Dir. Pen. Uomo*, 2019

Bonfanti A., Big data *e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *MediaLaws*, 3/2018

Bouchard C., *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. Ita. Dir. e Proc. Pen.*, 4/2019

Brennan-Marquez K., *Big Data Policing and the Redistribution of Anxiety*, in *Ohio State Journal of Criminal Law,* 2018

Canzio G., *Intelligenza artificiale, algoritmi e giustizia penale,* in *Sistema penale*, 8 gennaio 2021

Caplan J.M., Kennedy L.W., Barnum J.D., Piza E.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(2), 2017

Caplan J.M., Kennedy L.W., Piza E.L., *Risk Clusters, Hotspots and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies*, in *Journal of Quantitative Criminology*, 2010

Caplan J.M., Kennedy L.W., *Risk Terrain Modeling: Crime Prediction and Risk Reduction***,** Univ. of California Press, 2016

Cappellini A., *Profili penalistici delle* self-driving cars, in *Dir. Pen. Cont.*, 2/2019

Climer N., *Il cloud e l'Internet delle cose*, in J. Al-Khalili (a cura di), *Il futuro che verrà*, Bollati Boringhieri, 2017
Contissa G., Lasagni G., Sartor G., *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di internet*, 4/2019

De Hert P., Papakonstantinou V., *The new Police and Criminal Justice Data Protection Directive. A first Analysis*, in *New Journal of European Criminal Law*, 1/2016

De Tullio M.F., *La privacy e i* big data *verso una dimensione costituzionale collettiva*, in *Pol. dir.*, 2016

Donini M., Papa M. (a cura di), *Diritto penale del nemico. Un dibattito internazionale*, Giuffrè, 2007

Dwivedi V., Pattanaik V., Deval V., Dixit A., Norta A., Draheim D., *Legally Enforceable Smart-Contract Languages: A Systematic Literature Review*, in *ACM Computing Surveys*, Vol. 54, n. 5, 2020

Ferguson A.G., *Predictive Policing and Reasonable Suspicion*, in *Emory Law Journal*, Vol. 67, Issue 2, 2012

Ferrajoli L., *Il diritto penale del nemico e la dissoluzione del diritto penale*, in *Questione Giustizia*, 2006

Fronza E., "*Code is Law". Note a margine del volume di Antoine Garapon e Jean Lasségue, Justice digitale. Révolution graphique et rupture anthropologique, PUF, Paris, 2018*, in *Dir. Pen. Cont.*, 11 dicembre 2018

Garapon A., Lasségue J., *Justice digitale. Révolution graphique et rupture anthropologique*, PUF, Paris, 2018

Gerber M.S., *Predicting crime using Twitter and kernel density estimation*, in *Decision Support Systems*, Vol. 61, 2014

Gialuz M., *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Dir. Pem. Cont.,* 2019

Giannini A., *Lombroso 2.0: On AI and Predictions of Dangerousness in Criminal Justice*, in *RIDP*, Vol. 29, Issue 1, 2021

Giraldi L., *Intelligenza artificiale e* predictive policing *nella rinnovata fase di indagine*, in A. Massaro (a cura di), *Intelligenza artificiale e giustizia penale*, Paruzzo, 2020, 39-92

Grossi L., Software *predittivi e diritto penale*, in A. Massaro (a cura di), *Intelligenza artificiale e giustizia penale*, Paruzzo, 2020, 162-170

Hassan S., De Filippi P., *The expansion of algorithmic governance: From code is law to law is code*, in *Field Actions Science Report*, Special Issue, 17, 2017

Hildebrandt M., *Code driven law. Freezing the future and scaling the past*, in C. Markou, S. Deakin (a cura di), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence*, Bloomsbury Publishing, 2020.

Hildebrandt M., *Legal and technological normativity: more (and less) than twin sisters*, in *Technè: Research in Philosophy and Technology*, 12/2008

Illuminati G., *Editoriale*, in *Rev. italo-española der. proc.*, 1/2019

Irti N., *Per un dialogo sulla calcolabilità giuridica,* in *Riv. Dir. Proc.*, 2016; A. Carleo (a cura di), *Calcolabilità giuridica*, Il Mulino, 2017

Joh E.E., *Policing the smart city*, in *International Journal of Law in Context*, 15/2019.

Lavorgna A., Stuffia G., *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale: un passo necessario, ma non sufficiente, nella giusta direzione*, in *Dir. Pen. Cont.*, 2/2021

Lessig L., *Code and Other Laws of Cyberspace*, Basic books, 1999

Lessig L., *Code is law. On Liberty in cyberspace,* in *Harvard Magazine*, 2000

Liao S.H., Chu P.H., Hsiao P.H., *Data Mining Techniques and Applications – A decade review from 2000 to 2011*, in *Expert Systems and Applications*, 39, 2012

Lum K., Isaac W., *To Predict and Serve?,* disponibile all'indirizzo **https://doi.org/10.1111/j.1740-9713.2016.00960.x**

Maestri E., Lex informatica *e diritto. Pratiche sociali, sovranità e fonti nel* cyberspazio, in *Il Mulino Riv. web*, n. 1/2017

Manes V., *Intelligenza artificiale e giustizia penale*, in U. Ruffolo (a cura di), *XXVI Lezioni di diritto dell'Intelligenza Artificiale*, Giappichelli Editore, 2021

Manes V., *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020

Mantovani F., *Diritto penale. Parte generale*, 11a ed., Cedam, 2020

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

Mattern S., *Mission control: A history of the urban dashboard*, in *Places Journal*, 2015

Mazzacuva N., *Il disvalore di evento nel diritto penale*, Giuffrè, 1983

Palazzo F., *Contrasto al terrorismo, diritto penale del nemico e diritti fondamentali*, in *Questione giustizia*, 2/2006

Palazzo F., *La recente legislazione penale*, Cedam, 1985

Papa M., *Fantastic voyage. Attraverso la specialità del diritto penale*, 2a ed., Giappichelli Editore, 2019

Papa M., *Future Crimes: intelligenza artificiale e rinnovamento del diritto penale,* in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini Giuridica, 2020

Papa M., *La fattispecie come sceneggiatura dell'ingiusto: ascesa e crisi del diritto penale cinematografico*, in *Criminalia*, vol. 2019

Parodi C., Sellaroli V., *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Dir. Pen Cont.*, 6/2019, 56.

Pelliccia R., *Polizia predittiva: il futuro della prevenzione criminale?*, in *www.cyberlaws.it*, 9 maggio 2019

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

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.*, 18 dicembre 2018

Quattrocolo S., *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 3/2020

Riccio G., *Ragionando su intelligenza artificiale e processo penale*, in *Arch. pen.*, 3/2019

Sajfert J., Quintel T., *Data Protection Directive (EU) 2016/680 for police and criminal justice authorities*, in M. Cole, F. Bohem (a cura di*), GDPR Commentary*, Edward Elgar Publishing Ltd., 2018

Sarra C., Business Intelligence *ed esigenze di tutela: criticità del c.d.* Data Mining, in P. Moro, C. Sarra (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, FrancoAngeli, 2017

Seidensticker K., Bode F., Stoffel F., *Predictive Policing in Germany*, Projekt SKALA, 2018, disponibile all'indirizzo http://nbn-resolving.de/urn:nbn:de:bsz:352-2-14sbvox1ik0z06

Sgubbi F., *Il diritto penale totale*, Il Mulino, 2019, 41 ss.

Sgubbi F., *Il reato come rischio sociale. Ricerche sulle scelte di allocazione dell'illegalità penale*, Il Mulino, 1990

Simoncini A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà,* in *BioLaw Journal,* 2019

Sorbello P., *Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto*, in *Dir. pen. cont.*, 2/2019

Tulumello V.S., Iapaolo F., *Policing the future, disrupting urban policy today. Predictive policing, smart city and urban policy in Memphis (TN)*, in *Urban Geography*, 2019.

Ubertis F., *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. Pen. Cont.*, 4/2020

Venturi M., KeyCrime – *La chiave del crimine*, in *PrimoPiano*, 12/2014, disponibile su www.onap-profiling.org

Williams F.P., Mc Shane M.D., *Devianza e criminalità*, Il Mulino, 2002