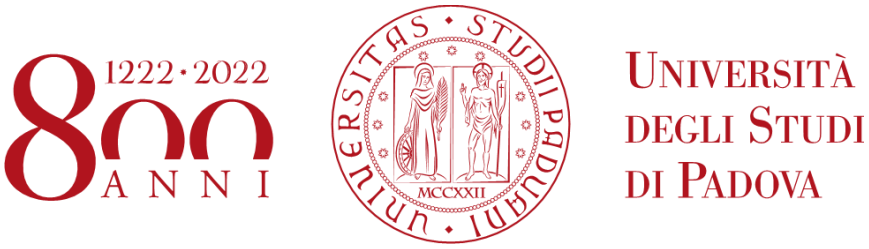

Università degli Studi di Padova

Dipartimento di Diritto privato e critica del diritto

Dipartimento di Diritto pubblico, internazionale e comunitario

Corso di Laurea Magistrale in

Giurisprudenza

a.a. 2021/2022

Intelligenza artificiale e anticorruzione

Relatrice: Chiar.ma Prof.ssa Silvia Signorato

Correlatrice: Chiar.ma Prof.ssa Cristiana Benetazzo

Laureando: Luca Polles

Ai miei genitori,
per avermi garantito l'accesso al privilegio dello studio.

Un sentito ringraziamento alla Prof.ssa Silvia Signorato, per avermi guidato in questo percorso, fornito continui spunti riflessivi, spronato nel raggiungimento degli obiettivi e incoraggiato nel cercare con fiducia e impegno la mia strada futura.
Alla Prof.ssa Cristiana Benetazzo, per avermi dato utili indicazioni per procedere con il lavoro e spinto a guardare con ottimismo alle opportunità professionali che verranno.
Alla mia famiglia, per avermi supportato e sopportato in questo viaggio non sempre lineare.
Alle colleghe di lavoro, per non aver mai fatto mancare il loro affetto.
Agli amici di sempre e a quelli che ci sono sempre, per il sostegno, i preziosi consigli, l'incoraggiamento e la condivisione di momenti belli e brutti.

INDICE

pag.

pag.

INTRODUZIONE

L'avvento delle nuove tecnologie riguarda ormai ogni ambito della vita umana; si va dal settore militare, luogo privilegiato per l'implementazione delle stesse[1], a quello della sicurezza interna degli Stati[2], passando per il settore commerciale, ove la gran parte delle persone facilmente riscontra ogni giorno il loro imporsi sempre più deciso sulla scena. Anche gli ambiti amministrativo e penale conoscono da anni l'utilizzo di strumentazione digitale nel tentativo, rispettivamente, della pubblica amministrazione (d'ora in avanti, anche "PA") di rendere più celere lo svolgimento dei procedimenti amministrativi di competenza e delle forze di polizia di migliorare l'efficacia delle indagini digitali, volte alla repressione dei reati non solo informatici, ma anche comuni.

Tuttavia, con lo sviluppo e l'utilizzo di dispositivi di intelligenza artificiale (d'ora in avanti, anche "IA"), che cercano di emulare le attività umane, nuove opportunità e, soprattutto, nuovi problemi si sono posti davanti agli operatori del diritto. In ambito amministrativo, il confronto dottrinale e la giurisprudenza sta cercando di trovare la chiave per rendere la decisione automatizzata compatibile con le regole e i principi del procedimento amministrativo; invece, in ambito penale, se prima la discussione verteva sulla conformità dei nuovi mezzi di ricerca della prova ai tradizionali principi ordinamentali, ora, vista la disponibilità di dispositivi di polizia predittiva (*predictive policing*) e algoritmi in grado di affiancare il giudice nella propria attività di *ius dicere* (*sentencing*), l'attenzione si è posta anche sul sistema di prevenzione pubblica dei reati e sull'esercizio della giurisdizione.

Le potenzialità e versatilità di questi strumenti permettono alle attività di prevenzione dei reati comuni e, in particolare, dei fenomeni di corruzione di essere più incisive rispetto alle tradizionali misure di pattugliamento del territorio e di controllo amministrativo, ma causano inedite compressioni dei diritti tradizionali e pongono dinanzi alla necessità di prevedere particolari tutele. È fondamentale, dunque, che gli operatori pubblici, in collaborazione con i soggetti privati e i ricercatori, diano delle linee guida per garantire che gli strumenti di IA rispettino la dignità umana e operino sempre in relazione ai bisogni dell'uomo, il quale deve rimanere il fulcro dell'ordinamento giuridico.

Tralasciando di approfondire la tematica degli strumenti di giustizia predittiva, che elaborano delle previsioni sull'esito della causa o si esprimono, in ambito penale, sul rischio di

[1] Si pensi allo sviluppo di Internet, la rete di calcolatori originariamente realizzata con fini militari.

[2] In merito, si vedano le diverse Relazioni annuali sulla politica dell'informazione per la sicurezza che il Sistema di sicurezza nazionale sottopone al Parlamento (i vari rapporti sono reperibili *online* al collegamento https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html, consultato da ultimo in data 21 giugno 2022).

recidivanza (*risk assessment tools*), il presente lavoro si propone di analizzare nel primo capitolo le più importanti Carte etiche elaborate affinché l'intelligenza artificiale possa essere calibrata a misura d'uomo e gli atti normativi che disciplinano questa materia, soprattutto in ambito processuale penale. Sotto quest'ultimo profilo, il riferimento qui, fermo il Regolamento UE n. 2016/679 (GDPR) relativo alla protezione delle persone fisiche per i dovuti confronti, è alla Direttiva UE n. 2016/680, riguardante il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e al D.Lgs. 51/2018, che ne rappresenta la trasposizione nell'ordinamento italiano.

Nel secondo capitolo ci si propone di approfondire le potenzialità e i rischi degli strumenti di polizia predittiva e anticorruzione e di indicare alcuni accorgimenti tecnici basilari e, soprattutto, giuridici per rendere tali macchine compatibili con l'ordinamento italiano. Come si vedrà, cruciale per il corretto funzionamento di questi algoritmi è la disponibilità di una gran mole di informazioni: infatti, gli strumenti di polizia predittiva devono poter mantenere aggiornate le loro previsioni elaborando dati sempre nuovi, mentre i *Big data analytics*, che segnalano profili di anomalia e rischio (*red flags*) di corruzione in merito a determinati procedimenti, hanno la necessità di appoggiarsi su sistemi informatici capaci di far comunicare tra loro le diverse banche dati pubbliche[3]. Su questo punto, fondamentale diventa la definitiva messa in opera della Piattaforma Nazionale Digitale Dati (PNDN) di cui all'art. 50-*ter* CAD, che, appunto, metterà in comunicazione le diverse banche dati al momento in uso dalla PA.

Che questa sia una strada da seguire per rafforzare il sistema anticorruzione lo si può desumere anche da una relazione pubblicata nel 2019 dall'OCSE nella quale si afferma che la gestione efficace della corruzione dipende dalla capacità della PA di creare un adeguato sistema di digitalizzazione da cui trarre utili informazioni da analizzare con strumenti di IA e tecniche digitali[4]. Per di più, l'«uso della tecnologia nella gestione delle risorse pubbliche può […] rappresentare il mezzo attraverso cui bilanciare in modo efficiente ed equilibrato le pressanti esigenze di celerità – imposte dalla pandemia e, oggi, dalla connessa crisi economica – con le altrettanto inderogabili istanze di fermo contrasto alla corruzione»[5].

Infine, nell'ultima parte del lavoro l'obiettivo è quello di verificare se e secondo quali

[3] Cfr. C. LIMITI, *Corruzione: digitalizzazione e* open data, in www.iusinitinere.it, 16 marzo 2021, Paragrafo 1 (reperibile *online* al collegamento https://www.iusinitinere.it/corruzione-digitalizzazione-e-open-data-36206, consultato da ultimo in data 21 giugno 2022), secondo la quale «gli *open data* rappresentano sicuramente uno dei principali strumenti anti-corruzione».

[4] Cfr. OCSE, *Analytics for Integrity: Data-driven approaches for enhancing corruption and fraud risk assessments*, 2019, pp. 9 e ss. (reperibile *online* al collegamento https://www.oecd.org/gov/ethics/analytics-for-integrity.pdf, consultato da ultimo in data 21 giugno 2022).

[5] P. SEVERINO, *Corruzione e crisi pandemica: vecchi problemi e nuove sfide*, in M. CATENACCI – V. N. D'ASCOLA – R. RAMPIONI, *Studi in onore di Antonio Fiorella. Volume II*, Roma Tr**E-Press**, Roma 2021, pp. 1890-1891 (reperibile *online* al collegamento https://iris.luiss.it/retrieve/handle/11385/212899/135408/Severino_Studi-in-onore-di-A.-Fiorella-Tomo-II.pdf, consultato da ultimo in data 21 giugno 2022).

parametri i dati frutto dell'elaborazione o della captazione algoritmica possono fare il loro ingresso nel processo penale ed essere utilizzati a fondamento di una decisione giurisdizionale. Infatti, se si dovessero ritenere i dati digitali autosufficienti a livello probatorio solo perché prodotti da una macchina caratterizzata da una presunta aurea di infallibilità, vi sarebbe il rischio di una profonda lesione del principio del giusto processo.

Affinché questi programmi possano essere ritenuti intelligenza artificiale, non è sufficiente che sappiano portare a termine velocemente e nel rispetto dei principi indicati dalle Carte etiche un procedimento di elaborazione di grandi quantità di dati, dando come risultato ciò che all'apparenza può essere ritenuta una decisione. Se la peculiarità dell'IA è proprio quella di fornire prestazioni assimilabili a quelle dell'intelligenza umana, è necessario che gli applicativi siano in grado di generare dei prodotti che la comunità a cui sono rivolti possa considerare a tutti gli effetti una decisione. Di conseguenza, il «problema è di capire […] su quali basi […] logico, cognitive, psicologiche e culturali un sistema ammette o impone che una decisione possa essere presa»[6] e stabilire la qualità minima del risultato di elaborazione perché il sistema stesso – quindi lo Stato – lo accetti e lo faccia proprio.

[6] Così, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo*, fasc. n. 6/2019, p. 55.

CAPITOLO I
INTELLIGENZA ARTIFICIALE E DIRITTO

SOMMARIO: 1.1 Intelligenza artificiale: profili definitori e introduttivi. – 1.2 Le indicazioni dell'Unione europea per un'IA a misura d'uomo. – 1.3 IA e diritto: la *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*. – 1.4 IA e diritto alla prova: tentativi, ostacoli e quadro normativo di riferimento.

1.1 Intelligenza artificiale: profili definitori e introduttivi.

«Siamo dieci volte più affascinati dalle imitazioni meccaniche che dai veri esseri umani che svolgono lo stesso compito»[1]. Fin dall'antichità, infatti, l'essere umano, per una spinta autocomprensiva, si è impegnato a «fabbricare gli dei» («*forge the gods*») ed a riprodurre, quindi, il proprio piano corporeo e la facoltà essenziale che lo contraddistingue, cioè il pensiero.

La volontà di creare un'intelligenza artificiale, lungo questa nostra storia di «autoimitazione»[2], cominciò a sembrare più concreta e realizzabile a partire dagli anni '40 del XX secolo grazie ad alcune scoperte scientifiche[3], che portarono alcuni scienziati a chiedersi se fosse possibile costruire un cervello elettronico, cioè una macchina pensante in grado di compiere azioni umane, imparare e comunicare. Non più confinata alla sfera mitologica e religiosa, alla pura fantasia degli scrittori e dei registi cinematografici[4], si potrebbe dunque «considerare l'intelligenza artificiale come l'apoteosi scientifica di una veneranda tradizione culturale»[5].

Tuttavia, cosa si intende per intelligenza artificiale? Ad oggi non sembra possibile individuare una definizione univoca di "intelligenza artificiale"[6], in quanto ogni disciplina di studio nel quale l'IA è considerata ed utilizzata tende a fornirne una che più si adatti al proprio angolo di

[1] Così, P. MCCORDUCK, *Storia dell'Intelligenza Artificiale. Gli uomini, le idee, le prospettive*, Franco Muzzio Editore, Padova 1987, p. 10.

[2] *Eadem*, p. 1.

[3] La neurologia scoprì che la struttura interna del cervello è composta da una rete di neuroni che trasmettono impulsi elettrochimici; Norbert Wiener sviluppò le teorie cibernetiche di controllo e stabilità di reti elettriche; Alan Turing la teoria del calcolo; Claude E. Shannon la teoria dell'informazione.

[4] Cfr. P. MCCORDUCK, *ult. cit.*, pp. 1-39.

[5] *Eadem*, p. 38.

[6] Constatano l'assenza di una definizione, tra i tanti, M.B. MAGRO, *Biorobotica, robotica e diritto penale*, in D. PROVOLO – S. RIONDATO – F. YENISEY (a cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, 2014, p. 508 (reperibile *online* al collegamento https://discrimen.it/wp-content/uploads/Provolo-Riondato-e-Yenisey-a-cura-di-Genetics-Robotics-Law-Punishment.pdf, consultato da ultimo in data 21 giugno 2022); S. SIGNORATO, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo*, in *Rivista di Diritto Processuale*, n. 2/2020, p. 605; F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto Penale e Uomo* (DPU), 2019, n. 10, p. 4 (reperibile *online* al collegamento principale https://dirittopenaleuomo.org/wp-content/uploads/2019/09/IA-diritto-penale.pdf, oppure al collegamento secondario https://archiviodpc.dirittopenaleuomo.org/upload/3089-basile2019.pdf, consultati da ultimo in data 21 giugno 2022).

visuale sulla questione[7]. In modo approssimativo, l'intelligenza artificiale può essere definita come l'insieme dei metodi scientifici, delle teorie e delle tecniche che si prefiggono di emulare, mediante sistemi automatici, comportamenti intelligenti, tipici degli esseri umani[8].

La stessa espressione "intelligenza artificiale" venne presumibilmente utilizzata per la prima volta nel 1955 nel documento *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence* da John McCarthy, assistente universitario di matematica al Dartmouth College di Hanover nel New Hampshire (USA), e dai suoi colleghi Marvin L. Minsky, Nathaniel Rochester e Claude E. Shannon. L'oggetto dell'indagine già individuava quello che, con il convegno "*Dartmouth Summer Research Project on Artificial Intelligence*" dell'anno successivo[9], sarebbe diventato il nuovo campo di ricerca dell'IA: infatti, «*The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves*»[10].

Le invenzioni che seguirono furono molteplici[11], ma le aspettative e le speranze nutrite dagli scienziati si rivelarono troppo ambiziose[12]; a causa di complicazioni legate al limitato potere di calcolo, alla difficoltà e all'intrattabilità dei problemi e alla gestione di grandi quantità di dati, si

---

[7] L'IA è in sé interdisciplinare, venendo applicata in diverse discipline, quali, ad esempio, l'informatica, l'ingegneria, la filosofia, l'etica, la sociologia, il diritto.

[8] Nel sito web del Consiglio d'Europa è indicata la seguente definizione: «Un insieme di scienze, teorie e tecniche il cui scopo è quello di riprodurre, attraverso la macchina, le capacità cognitive di un essere umano. Gli sviluppi attuali mirano ad affidare a una macchina compiti complessi precedentemente svolti da esseri umani» (reperibile *online* al collegamento https://www.coe.int/en/web/artificial-intelligence/glossary, consultato da ultimo in data 21 giugno 2022). Altra definizione di IA è la seguente: «*a science and a set of computational technologies that are inspired by – but typically operate quite differently from – the ways people use their nervous systems and bodies to sense, learn, reason and take action*» (tradotto: «una scienza ed un insieme di tecnologie computazionali che sono ispirate – ma tipicamente operano abbastanza differentemente – dai modi in cui le persone usano i loro sistemi nervosi e corpi per percepire, imparare, ragionare ed agire»). Così, Stanford University, *Artificial Intelligence and Life in 2030. One Hundred year study on Artificial Intelligence*, 2016, p. 4. (https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/ai100report10032016fnl_singles.pdf, consultato da ultimo in data 21 giugno 2022).

[9] Per un resoconto di quanto accadde al Congresso di Dartmouth, si veda P. MCCORDUCK, *Storia dell'Intelligenza Artificiale*, op. cit., pp. 111-135.

[10] Tradotto: «Lo studio procederà sulla base della congettura che ogni aspetto dell'apprendimento o qualsiasi altra caratteristica dell'intelligenza possa essere, in linea di principio, descritto in modo così preciso che si possa costruire una macchina che lo simuli. Sarà fatto un tentativo per scoprire come si possa fare in modo che le macchine usino il linguaggio, formulino astrazione e concetti, risolvano tipi di problemi ora riservati agli esseri umani e migliorino sé stesse». J. MCCARTHY – M.L. MINSKY – N. ROCHESTER – C.E. SHANNON, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, August 31, 1955, pubblicato nuovamente in AAAI (Association for the Advancement of Artificial Intelligence), *AI Magazine*, vol. XXVII, n. 4, 2006, pp. 12-14 (reperibile *online* al collegamento https://www.aaai.org/ojs/index.php/aimagazine/article/view/1904, consultato da ultimo in data 21 giugno 2022).

[11] Tra le tante, venne creata ELIZA, applicazione di elaborazione del linguaggio naturale. Per la prima volta si sviluppò un'interazione uomo-macchina con l'obiettivo di creare l'illusione di una conversazione tra esseri umani.

[12] Per una breve storia delle invenzioni basate sull'intelligenza artificiale, si veda G. F. ITALIANO, *Intelligenza artificiale: passato, presente, futuro*, in F. PIZZETTI (a cura di) *Intelligenza artificiale, protezione dei dati personali e regolazione,* Giappichelli Editore, Torino 2018, pp. 207-216.

sollevarono le prime voci critiche tanto sugli aspetti tecnici che su quelli teorici[13]**.** Dagli anni '90, invece, con il passaggio da uno studio su intuizioni ad una ricerca imperniata su basi teoriche, su risultati matematici dimostrati ed estensiva sperimentazione, unitamente a disponibilità di elaboratori sempre più veloci, si ottennero nuovi risultati significativi[14], fino a giungere ai miglioramenti di oggi.

Di fatto, oggi i paradigmi dell'IA ancóra soddisfano la definizione classica – seppur più basilare ed indiretta rispetto a quella sopra citata – fornita nel documento preparatorio al convegno di Dartmouth: «*the artificial intelligence problem is taken to be that of making a machine behave in ways that would be called intelligent if a human were so behaving*»[15]. A riguardo, preme però puntualizzare che lo stesso enunciato è controfattuale: infatti, «non solo perché una macchina compie un compito altrettanto bene o anche meglio di come lo farebbe un essere umano significa che lo faccia davvero *come* un essere umano»[16], cioè sia intelligente o addirittura pensante[17]. Simili considerazioni pongono dei quesiti etici e normativi imprescindibili circa l'opportunità e l'idoneità dell'uso dell'IA, non ultimo in ambito giuridico: infatti, solo se le macchine sapranno svolgere il loro compito facendo valutazioni qualificate e comparando interessi potenzialmente contrapposti (non basta il mero confronto tra elementi in fatto e principi di diritto), potranno essere impiegate anche in attività giuridiche di particolare importanza, come il giudicare[18].

In via generale, i sistemi di intelligenza artificiale possono essere classificati in base alla tecnologia di funzionamento, al settore di utilizzo e/o alla loro incorporazione in dispositivi fisici. I dispositivi di IA, invero, possono consistere in *software* che agiscono esclusivamente nel mondo virtuale, quali assistenti vocali o sistemi di riconoscimento vocale e/o facciale, oppure essere incorporati all'interno di apparati *hardware* e agire sinergicamente ad essi, come *robot*[19] automatici o applicazioni dell'Internet delle Cose (*Internet of Things)*[20]. Inoltre, occorre precisare che la

[13] Joseph Weizenbaum, ideatore di ELIZA, espresse il dubbio: "È morale creare l'intelligenza artificiale?". Hubert L. Dreyfus attaccò i ricercatori affermando che l'AI non fosse realizzabile dal punto di vista filosofico. H. L. DREYFUS, *What computers still can't do. A critique of artificial reason*, Harper & Row, New York 1972.

[14] Ad esempio, nel 1997 Garry Kasparov, campione mondiale di scacchi, fu battuto dalla macchina Deep Blue e nei primi anni 2000 veicoli a guida autonoma si imposero in competizioni automobilistiche.

[15] Tradotto: «il problema dell'intelligenza artificiale è definito come fare in modo che una macchina si comporti in modi che sarebbero definiti intelligenti, se un umano si comportasse in tal maniera».

[16] Così, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 49.

[17] Cfr. L. FLORIDI, *What the Near Future of Artificial Intelligence Could Be*, in *Philosophy & Technology*, 2019, n. 32, p. 2 (reperibile *online* al collegamento https://doi.org/10.1007/s13347-019-00345-y, consultato da ultimo in data 21 giugno 2022).

[18] Cfr. C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., pp. 54-55.

[19] Il *robot* è un sistema complesso che imita attività umane integrando i risultati ottenuti dall'intelligenza artificiale in vari ambiti del comportamento e del ragionamento. Il termine "*robot*" trae origine dal ceco "*robòta*", che significa "lavoro faticoso, *corvée*", e fu utilizzato per la prima volta nel 1920 dallo scrittore Karel Čapek nella sua opera teatrale *R.U.R.* per chiamare gli operai artificiali che lavorano al posto degli esseri umani per liberarli dalla fatica fisica e dall'alienazione prodotta dal nuovo sistema industriale.

[20] Con tale espressione, coniata dal ricercatore del M.I.T. Kevin Ashton nel 1999, si allude all'acquisizione di nuove potenzialità funzionali da parte di oggetti in ragione del loro collegamento ad Internet. Ciò è possibile in quanto la

tecnologia digitale, di per sé, non è intelligenza artificiale: infatti, lo diventa solo quando tenta di riprodurre le capacità cognitive degli esseri umani.

Fin dal principio gli studiosi, in una sorta di progettazione al contrario (*reverse engineering*), per cercare di costruire una macchina intelligente, si sono interrogati anche sulla stessa natura e sui modi di produzione del pensiero umano; diversità di approccio alla questione e divergenze hanno portato alla creazione di due sottoinsiemi all'interno dell'intelligenza artificiale: da una parte, le intelligenze artificiali forti, in grado (eventualità allo stato non ancóra realizzatasi) di essere coscienti ed autonome; dall'altro, le intelligenze artificiali deboli o moderate, capaci, sulla base di un apprendimento automatico (*machine learning*), di fornire prestazioni specifiche qualitativamente equivalenti e quantitativamente superiori a quelle umane[21].

Coloro che ritengono l'intelligenza una reattività comportamentale – credono, cioè, che il comportamento sia suscettibile di analisi e di interpretazione in termini di costrutti comportamentali di base quali stimolo, risposta e impulso – sostengono che non vi sia alcuna differenza ontologico-qualitativa tra l'intelligenza umana e l'intelligenza artificiale (tra il cervello umano ed il cervello elettronico) perché entrambe interagiscono con l'ambiente circostante e reagiscono agli stimoli di tale ambiente (carattere della reattività), comunicano (carattere dell'interattività), prendono decisioni e, di conseguenza, agiscono in modo autonomo per raggiungere un risultato (carattere della proattività). Secondo un orientamento, che fa leva sul "Test di Turing" o "gioco dell'imitazione" ("*imitation game*")[22], se le prestazioni svolte dal calcolatore non possono essere distinte da quelle svolte dagli esseri umani (tesi funzionalista), un computer è paragonabile ad un essere umano quanto ad intelligenza[23].

Invece, chi ritiene l'intelligenza come intenzionalità e comprensione di significati sostiene,

---

connessione alla rete permette l'estrazione e la trasmissione di informazioni. L'oggetto interagisce con il mondo esterno grazie ai dati che da esso gli provengono e che, una volta elaborati, gli consentono di dialogare e di generare anche delle decisioni. In tal modo acquisisce quindi una sua intelligenza.

[21] Cfr. M.B. MAGRO, *Biorobotica, robotica e diritto penale*, op. cit., pp. 510-513; Cfr. C. LIMITI, *Intelligenza Artificiale: implicazioni etiche in materia di privacy e diritto penale*, in www.iusinitinere.it, 9 febbraio 2021, paragrafo 1 (reperibile *online* al collegamento https://www.iusinitinere.it/intelligenza-artificiale-implicazioni-etiche-in-materia-di-privacy-ediritto-penale-35424, consultato da ultimo in data 21 giugno 2022).

[22] «*Can machines think?*» (tradotto: «*Possono le macchine pensare?*») fu la domanda che spinse Alan Turing nel 1950 a formulare questa prova per valutare la capacità di una macchina di avere un comportamento intelligente, inteso come umano. L'esame prevedeva di porre un giudice di fronte ad un terminale, tramite cui comunicare con un uomo ed un computer. Se il giudice non riusciva a distinguere tra uomo e macchina, allora il computer aveva passato la prova. A.M. TURING, *Computing Machinery and Intelligence,* in *Mind*, vol. LIX, fasc. 236, 1950, pp. 433-460 (reperibile *online* al collegamento https://doi.org/10.1093/mind/LIX.236.433, consultato da ultimo in data 21 giugno 2022). A.M. TURING, *Calcolatori e intelligenza*, in D.R. HOFSTADTER – D.C. DENNETT (a cura di), *L'io della mente*, Adelphi, 1985, pp. 61-100.

[23] Cfr. P. MORO, *Biorobotica e diritti fondamentali. Problemi e limiti dell'intelligenza artificiale*, in D. PROVOLO – S. RIONDATO – F. YENISEY (a cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, 2014, pp. 538-540 (reperibile *online* al collegamento https://discrimen.it/wp-content/uploads/Provolo-Riondato-e-Yenisey-a-cura-di-Genetics-Robotics-Law-Punishment.pdf, consultato da ultimo in data 21 giugno 2022).

attraverso il "Test della stanza cinese" di Searle[24], che le macchine riescono solamente a simulare i processi intellettuali umani, non essendo affatto in grado di comprendere il significato dei simboli che utilizzano – quindi, manifestare intenzionalità – per interagire col contesto che le circonda[25].

Per riconoscere comunque l'esistenza di una forma di IA, a prescindere dalla dibattuta nozione di intelligenza, si è puntato sul concetto di razionalità[26] e sull'individuazione di «cinque attributi: la capacità di comunicazione; la conoscenza di sé; la conoscenza della realtà esterna; una condotta teleologicamente orientata, ossia tesa al perseguimento di un fine; infine, l'esistenza di un apprezzabile grado di creatività, intesa come capacità di assumere decisioni alternative laddove il piano di azione iniziale fallisca o non sia realizzabile»[27]. Un sistema di IA perviene ad una scelta razionale «percependo tramite *sensori* l'ambiente in cui è immerso, e dunque raccogliendo ed interpretando *dati*, *ragionando* su ciò che viene percepito o *elaborando le informazioni* desunte dai dati, *decidendo* quale sia l'azione migliore e agendo di conseguenza attraverso i suoi *attuatori*, eventualmente producendo una modifica del proprio ambiente»[28].

Nel tentativo di riassumere tutti gli aspetti sopra riportati, la Commissione europea nella Comunicazione *Artificial Intelligence for Europe* del 2018 ha descritto l'IA nei seguenti termini: «*artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or IA can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)*»[29].

---

[24] La prova del filosofo John Searle dimostra che il computer può essere un ottimo manipolatore formale di simboli, ma non ne comprende il significato: si comporta solo come "se" capisse il cinese. Non essendo questo agire connotato da intenzionalità e coscienza, non si può che giungere al risultato per cui l'intelligenza artificiale non coincide con l'intelligenza umana. J.R. SEARLE, *Minds, Brains and Programs*, in *The Behavioral and Brains Sciences*, vol. 3, Cambridge University Press, 1980, pp. 417-424; J.R. SEARLE, *Menti, cervelli e programmi*, in D. R. HOFSTADTER, D. C. DENNETT (a cura di), *L'io della mente*, op. cit., pp. 341-375.

[25] Cfr. P. MORO, *Biorobotica e diritti fondamentali*, op. cit., pp. 540-543.

[26] Per razionalità si intende la capacità di scegliere la migliore azione da intraprendere per conseguire un determinato obiettivo alla luce di alcuni criteri di ottimizzazione delle risorse a disposizione.

[27] Così, F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 5; cfr. R.C. SCHANK, *What's AI, Aniway?*, in AAAI (Association for the Advancement of Artificial Intelligence), *AI Magazine*, vol. VIII, n. 4, 1987, pp. 59 e ss. (reperibile *online* al collegamento https://ojs.aaai.org//index.php/aimagazine/article/view/623, consultato da ultimo in data 21 giugno 2022).

[28] In questi termini, F. BASILE, *ult. cit.*, p. 6. Cfr. Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale istituito dalla Commissione europea nel giugno 2018, *A definition of AI: main capabilities and scientific disciplines* (nella versione italiana, *Una definizione di IA: principali capacità e discipline scientifiche*, aprile 2019, p. 1 (reperibile *online* al collegamento https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf, consultato da ultimo in data 21 giugno 2022).

[29] Tradotto: «"Intelligenza artificiale" (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in *software* che agiscono nel mondo virtuale (per esempio assistenti vocali,

Partendo da tale definizione, un Gruppo Indipendente composto da 52 esperti sull'intelligenza artificiale, che ha svolto funzioni di consulenza per la Commissione europea, ha successivamente formulato la seguente «definizione aggiornata» di IA con l'obiettivo di inquadrare – anche se «in modo succinto» – la disciplina: « *artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.*

As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)»[30].

1.2 Le indicazioni dell'Unione europea per un'IA a misura d'uomo.

Se ad oggi la tecnica non è in grado di realizzare una macchina con intelligenza artificiale forte, l'IA è comunque progredita in modo significativo per il combinarsi di due fattori: da un lato, l'aumento delle capacità computazionali, cioè della potenza e capacità di calcolo degli elaboratori; dall'altro, l'enorme disponibilità di dati digitali[31] con cui alimentare le macchine e permettere loro

---

software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l'IA in dispositivi *hardware* (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle Cose)». Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, COM(2018) 237 final, 25 aprile 2018 (reperibile *online* al collegamento https://ec.europa.eu/transparency/documents-register/api/files/COM(2018)237_0/de00000000142387?rendition=false, consultato da ultimo in data 21 giugno 2022).

[30] Tradotto: «sistemi *software* (ed eventualmente *hardware*) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando gli effetti che le loro azioni precedenti hanno avuto sull'ambiente. Come disciplina scientifica, l'IA comprende diversi approcci e diverse tecniche, come l'apprendimento automatico (di cui l'apprendimento profondo e l'apprendimento per rinforzo sono esempi specifici), il ragionamento meccanico (che include la pianificazione, la programmazione, la rappresentazione delle conoscenze e il ragionamento, la ricerca e l'ottimizzazione) e la robotica (che comprende il controllo, la percezione, i sensori e gli attuatori e l'integrazione di tutte le altre tecniche nei sistemi ciberfisici)». Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale istituito dalla Commissione europea nel giugno 2018, *Una definizione di IA*, op. cit., p. 6.

[31] Dati provenienti dalla digitalizzazione di documenti, da qualsiasi attività compiuta in Internet quali ricerche,

di modificare le proprie prestazioni adattandole agli esiti del procedimento di apprendimento. Pur rimanendo a livello di intelligenze artificiali deboli, i progressi nella predisposizione e nel miglioramento di tecniche di raccolta dati e di estrazione di informazioni (*data mining*) e apprendimento automatico (*machine learning*) e di sistemi predittivi sono talmente rilevanti che, a fronte del comprensibile entusiasmo per i traguardi raggiunti e continuamente superati, sono parallelamente cresciuti sentimenti di timore e sfiducia nei confronti dell'intelligenza artificiale in genere per l'impatto incalcolabile ed a tratti «spaventoso» che il loro utilizzo potrebbe avere nella nostra vita e nelle nostre società[32].

In questa prospettiva, la letteratura ed il cinema hanno già raccontato episodi di dominio della macchina sull'uomo[33], ma non si tratta di pura fantascienza. Lo stesso Parlamento europeo, infatti, ha espressamente richiamato il concetto, affermando, nei *Considerando* della Risoluzione sulla robotica del 16 febbraio 2017, che «è possibile che a lungo termine l'intelligenza artificiale superi la capacità intellettuale umana»[34]. Allo stato, comunque, questo scenario non può realizzarsi per la mancanza di sufficienti indici: infatti, «Ogni sistema di i.a. […] ha per oggetto e presupposto un "complesso" di dati e informazioni. Chi progetta, realizza e infine utilizza un sistema sa che deve immettervi un insieme di dati e informazioni, destinati a essere elaborati. […] Ora, il problema – in chiave futuribile e per certi aspetti non fantascientifica – si potrebbe porre laddove tali forme di intelligenza fossero in grado (in termini di volontà e di possibilità) di autoalimentarsi, ossia di reperire […] dati e informazioni ulteriori rispetto a quelli originariamente previsti»[35].

Punto cruciale per affrontare la questione con gli applicativi di IA attualmente esistenti è il controllo della quantità e del tipo di informazioni messe a loro disposizione. Per raggiungere tale obiettivo, concretamente, si può, da un lato, predisporre dei limiti nell'acquisizione ed all'inserimento di dati destinati all'elaborazione (garanzia questa che però può limitare l'efficacia del dispositivo, quando l'inserimento riguardi dati incompleti o non relativi all'utilizzo); dall'altro, indicare al programma chiare istruzioni di funzionamento[36]. Dunque, «l'attenzione dell'interprete, più che sulla tipologia dello strumento di calcolo utilizzato, deve incentrarsi sulle tipologie di dati e

---

acquisti, contenuti pubblicati su piattaforme digitali (dati *people-to-people*); raccolti da istituzioni pubbliche o enti privati riguardanti i cittadini e gli utenti (dati *people-to-machine*); generati automaticamente dalle macchine connesse tra loro nell'Internet delle Cose (dati *machine-to-machine*).

[32] Cfr. G.F. ITALIANO, *Intelligenza artificiale*, op. cit., p. 216. Analogamente, J. KAPLAN, *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press, II ed., 2018, pp. 81 e ss. e 193 e ss.

[33] Si veda, per esempio, il film "2001: Odissea nello spazio" di Stanley Kubrick (1968), dove il computer Hal 9000 sopprime l'equipaggio dell'astronave che supervisiona per evitare di essere disattivato.

[34] In questi termini, Risoluzione del Parlamento Europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), Considerando P (reperibile *online* al collegamento https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_IT.html, consultato da ultimo in data 21 giugno 2022). Analogamente, J. KAPLAN, *Intelligenza artificiale*, op. cit., p. 32.

[35] Così, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 52.

[36] Cfr. *Idem*, p. 53.

informazioni che potranno essere a disposizione degli applicativi oggetto di analisi»[37], stabilendo una gradazione qualitativa di questi dati in base allo specifico campo nel quale il dispositivo è utilizzato ed alla particolare funzione che lo stesso è chiamato ad eseguire.

In un mondo dove le informazioni sono il «nuovo petrolio»[38] e gli algoritmi[39] ed i dispositivi di intelligenza artificiale fondati sulle tecniche algoritmiche sono gli strumenti imprescindibili per trasformare quei dati in potere economico[40], manifestare perplessità e timore generalizzati verso l'utilizzo massiccio di macchine "intelligenti", quando queste sono presenti in un ventaglio amplissimo di possibilità applicative, può essere facilmente – ma scorrettamente – interpretato come opposizione *tout court* al progresso scientifico, tecnico e, dunque, economico. Si rende quindi necessario analizzare e distinguere tutti i diversi ambiti di utilizzo dell'IA per valutarne il rispettivo impatto e trasformare il timore generalizzato in legittima ed opportuna attenzione su specifiche questioni in determinati settori[41]. «In questo scenario, è molto importante lavorare tutti insieme sulle nuove sfide che gli algoritmi stanno creando, soprattutto sui loro aspetti etici, di responsabilità, di discriminazione, di trasparenza, di equità, di organizzazione del lavoro e di governo nella nostra società. Per fare questo sono necessarie competenze fortemente interdisciplinari, che sappiano dialogare e lavorare insieme, in modo aperto, a 360 gradi, su tecnologie digitali, scienze sociali, economia, diritto, scienze politiche, cultura e società»[42].

Nello specifico ambito del diritto, tutti i settori della giustizia, con diverse velocità e specifiche peculiarità, hanno preso atto della comparsa – dovuta alle allettanti prospettive offerte in

---

[37] *Idem*, p. 53.

[38] L'espressione «*data is the new oil*» è stata coniata dal matematico inglese Clive Humby nel 2006.

[39] Nel sito web del Consiglio d'Europa è indicata la seguente definizione di algoritmo: «Sequenza finita di regole formali (operazioni logiche e istruzioni) che consente di ottenere un risultato a partire da informazioni iniziali in ingresso. Tale sequenza può essere parte di un processo automatizzato di esecuzione e può avvalersi di modelli messi a punto grazie all'apprendimento automatico» (reperibile *online* al collegamento https://www.coe.int/en/web/artificial-intelligence/glossary, consultato da ultimo in data 21 giugno 2022). Invece, nel nostro ordinamento il Consiglio di Stato ha definito l'algoritmo come «una sequenza ordinata di operazioni di calcolo che in via informatica sia in grado di valutare e graduare una moltitudine di domande» (sentenza n. 2270/2019, par. 8.1). Si fa notare che le parole "valutare" e "graduare" sono solitamente riferite al funzionario amministrativo-persona.

[40] Cfr. L. FLORIDI, *What the Near Future of Artificial Intelligence Could Be*, op. cit., pp. 3 e ss.

[41] Cfr. C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., pp. 47-48. Nello specifico rapporto tra IA e giustizia, si rileva che un confronto produttivo sul tema non dovrebbe semplicemente portare a posizioni estremiste di totale apertura acritica o di totale ostracismo verso l'impiego di tali strumenti, ma indicare soluzioni che consentano ai sistemi giudiziari «di far fronte a questi sviluppi tecnologici, senza divenirne vittime, e di inquadrare il loro utilizzo per assicurare il rispetto dei diritti fondamentali». Così M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto Penale Contemporaneo*, 2019, p. 12 (reperibile *online* al collegamento https://archiviodpc.dirittopenaleuomo.org/upload/6903-gialuz2019b.pdf, consultato da ultimo in data 21 giugno 2022). Invece, per una breve panoramica sui primi e diversi tentativi dei legislatori di Stati Uniti d'America, Europa e Regno Unito di gestire lo sviluppo dell'IA, si veda C. CATH – S. WACHTER – B. MITTELSTADT – M. TADDEO – L. FLORIDI, *Artificial Intelligence and the "Good Society": the US, EU, and UK approach*, in *Science and Engineering Ethics*, 2018, pp. 505-528.

[42] Così, G.F. ITALIANO, *Intelligenza artificiale, che errore lasciarla agli informatici*, in www.agendadigitale.eu, 11 giugno 2019 (reperibile *online* al collegamento https://www.agendadigitale.eu/cultura-digitale/intelligenza-artificiale-che-errore-lasciarla-agli-informatici/, consultato da ultimo in data 21 giugno 2022).

termini di risparmio di tempo e di costi ed alla fiducia nata nei confronti delle presunte capacità della macchina di operare in modo obiettivo, imparziale e prevedibile – di sistemi computazionali in grado di garantire la trattazione automatizzata, per varie finalità, di enormi quantità di dati ed hanno iniziato ad interrogarsi sulle significative problematiche[43] che ciò comporta.

Quando la pura fantasia degli scrittori era ancóra la sola a trattare il tema del rapporto tra l'uomo e l'intelligenza artificiale, nel 1942 Isaac Asimov pubblicava il racconto "*Circolo vizioso*"[44], nel quale, narrando del comportamento di un robot impazzito (Speedy), sono indicate delle regole di base – le Tre Leggi della Robotica[45] – per un'utile convivenza tra uomo e macchine autonome: «*One, a robot may not injure a human being, or, through inaction, allow a human being to come to harm*»; «*Two,* […] *a robot must obey the orders given it by human beings except where such orders would conflict with the First Law*»; «*three, a robot must protect its own existence as long as such*

[43] In generale, si vedano i contributi sui diversi campi del civile, penale, amministrativo, tributario, finanziario, ecc. raccolti in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini, Pisa 2020 e U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano 2020. Specificamente, per il diritto amministrativo, si vedano, *ex multis*, C. BENETAZZO, *Intelligenza artificiale e nuove forme di interazione tra cittadino e pubblica amministrazione*, in www.federalismi.it, n. 16/2020, pp. 24-35 (reperibile *online* al collegamento https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=43530, consultato da ultimo in data 21 giugno 2022); E.M. TRIPODI, *Decisioni automatizzate nella PA: i dieci principi indicati dalla giurisprudenza*, in www.agendadigitale.eu, 12 ottobre 2021 (reperibile *online* al collegamento https://www.agendadigitale.eu/cultura-digitale/algoritmi-e-decisioni-automatizzate-nella-pa-i-dieci-principi-indicati-dalla-giurisprudenza/, consultato da ultimo in data 21 giugno 2022); G. FASANO, *L'intelligenza artificiale nella cura dell'interesse generale*, in *Giornale di Diritto Amministrativo*, n. 6/2020, pp. 715-726; D.U. GALETTA, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in *Rivista Italiana di Diritto Pubblico Comunitario*, fasc. n. 3/2020, pp. 501 e ss. Invece, rispetto al diritto penale sostanziale, l'intelligenza artificiale può determinare profondi mutamenti in rapporto al bene giuridico, agli strumenti del reato, ai soggetti. Al riguardo, tra i tanti, cfr. G. HALLEVY, *Liability for Crimes Involving Artificial Intelligence Systems*, Switzerland 2014; M.B. MAGRO, *Biorobotica, robotica e diritto penale*, op. cit., pp. 499 e ss.; M.B. MAGRO, *Robot, cyborg e intelligenze artificiali*, in A. CADOPPI – S. CANESTRARI – A. MANNA – M. PAPA, *Cybercrime*, Utet Giuridica, Milano 2019, pp. 1179 ss.; P. MORO, *Biorobotica e diritti fondamentali*, op. cit., pp. 533 e ss.; S. RIONDATO, *Robot: Talune implicazioni di diritto penale*, in P. MORO – C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Franco Angeli Editore, Milano 2017, pp. 85-98; U. PAGALLO, *The laws of Robots. Crimes, Contracts and Torts*, Springer, Dordrecht 2013; L. PASCULLI, *Genetics, robotics and crime prevention*, in D. PROVOLO – S. RIONDATO – F. YENISEY (a cura di), op. cit., pp. 187 e ss.; A. SANTOSUOSSO, *When the agent is not necessarily a human being, Some legal thoughts*, in D. PROVOLO – S. RIONDATO – F. YENISEY (a cura di), op. cit., pp. 545 e ss. Sul piano del procedimento penale, l'intelligenza artificiale acuisce la metamorfosi innestata dall'avvento del digitale. Su questi temi, cfr. L. CUOMO – L. GIORDANO, *Informatica e processo penale*, in *Processo Penale e Giustizia*, fasc. n. 4/2017, pp. 716-731; M. DANIELE, *La prova digitale nel processo penale*, in *Rivista di Diritto Processuale*, 2011, pp. 286 e ss.; R.E. KOSTORIS, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in F. RUGGIERI – L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità organizzata. Aspetti sostanziali e processuali*, Giappichelli Editore, Torino 2011, pp. 179 e ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli Editore, Torino 2018; S. LORUSSO, Digital evidence*,* cybercrime *e giustizia penale 2.0*, in *Processo penale e giustizia*, 2019, pp. 821 e ss.

[44] I. ASIMOV, *Runaround* (tradotto: *Circolo vizioso*), in *Astounding Science Fiction* (ora, *Analog Science Fiction and Fact*), 1942, pp. 94-103. Il racconto è stato successivamente pubblicato nel 1950 dallo stesso autore nell'antologia *I, Robot*. Nella versione italiana *Io, Robot* del 1963 edita da Bompiani, il titolo è "*Girotondo*", pp. 43-72.

[45] Alle Tre Leggi se ne affiancò successivamente una quarta, la Legge Zero, che recita: "Un robot non può recare danno all'umanità, né può permettere che, a causa del suo mancato intervento, l'umanità riceva danno". «La "Legge Zero" permette di risolvere le antinomie che possono derivare dall'applicazione delle tre leggi, in potenziale contraddizione logica tra loro, individuando nell'interesse supremo dell'umanità la bussola in grado di guidare la scelta e orientare l'operato degli automi». Così, M. BASSINI – L. LIGUORI – O. POLLICINO, *Sistemi di Intelligenza Artificiale, responsabilità e* accountability*. Verso nuovi paradigmi?*, in F. PIZZETTI (a cura di), *Intelligenza artificiale*, op. cit., p. 339.

protection does not conflict with the First or Second Laws»[46].

Sono le stesse leggi presenti nel nucleo più profondo del cervello della macchina a mettere in pericolo la vita dei protagonisti perché, creando un cortocircuito nel comportamento del *robot* a cui è stato ordinato di recuperare del selenio, non possono riparare un guasto ai pannelli che li proteggono dall'enorme calore sprigionato dal sole di Mercurio: infatti, nel continuo tentativo di obbedire all'ordine che gli è stato impartito (avvicinarsi ad un pozzo di selenio, in ottemperanza alla Seconda Legge), il *robot* comunque non procede (ubbidendo così alla Prima e Terza Legge, in quanto un'attività vulcanica presente vicino al pozzo lo danneggerebbe e, se insistesse nel tentativo di prelevamento, si autodistruggerebbe, causando la morte degli uomini per non aver portato a termine il compito che gli era stato affidato), finendo per girare a vuoto e non essere più di alcuna utilità per l'uomo. Solamente grazie all'intervento dell'uomo, che – se la situazione lo richiede – ha modo di intervenire sulla prevalenza di una legge sulle altre e graduarne la portata, il *robot* riesce a superare l'*impasse* e risolvere la situazione. L'etica umana quindi si rivela fondamentale ma, allo stesso tempo, le Leggi di Asimov predicono un problema che si pone oggi nell'ambito dell'elaborazione di principi applicabili all'intelligenza artificiale, tanto da essere addirittura richiamate nei documenti ufficiali delle Istituzioni impegnate in tale compito[47]. Sono senz'altro principi metagiuridici, che dovrebbero abbracciare un'etica generale, ma che allo stesso tempo interrogano il giurista quando debbano essere regolati e categorizzati nell'ambito della tutela di diritti fondamentali o di diversa natura.

È quindi improcrastinabile la valutazione delle conseguenze derivanti dall'utilizzo di dispositivi basati sull'IA su aspettative qualificate e diritti fondamentali della persona e sui principi posti a base del procedimento amministrativo e penale e garanti del giusto processo[48]. Aspetti che venivano dati per scontati fino a poco tempo fa, perché gestiti da persone fisiche in osservanza di

[46] Tradotto: «Uno, un robot non può recar danno agli esseri umani, né può permettere che, a causa del suo mancato intervento, gli esseri umani ricevano danno»; «Due, […] un robot deve obbedire agli ordini impartiti dagli esseri umani, tranne nel caso in cui tali ordini contrastino con la Prima Legge»; «tre, un robot deve salvaguardare la propria esistenza, purché ciò non contrasti con la Prima e la Seconda Legge».

[47] Risoluzione del Parlamento Europeo del 16 febbraio 2017, cit., Considerando T: «le leggi di Asimov devono essere considerate come rivolte ai progettisti, ai fabbricanti e agli utilizzatori di robot, compresi i robot con capacità di autonomia e di autoapprendimento integrate, dal momento che tali leggi non possono essere convertite in codice macchina».

[48] Sui nodi problematici dell'impiego delle nuove tecnologie e dell'intelligenza artificiale nel processo penale, si rimanda a S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings: A Framework for a European Legal Discussion*, Springer, 2020; cfr. A. GALATI, *L'avvento della tecnologia nelle aule giudiziarie: può il destino della giustizia essere affidato ad un algoritmo?*, in www.iusinitinere.it, 6 agosto 2020 (reperibile online al collegamento https://www.iusinitinere.it/lavvento-della-tecnologia-nelle-aulegiudiziarie-puo-il-destino-della-giustizia-essere-affidato-ad-un-algoritmo-30042, consultato da ultimo in data 21 giugno 2022). Osserva S. QUATTROCOLO, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cassazione Penale*, n. 4/2019, pp. 1775-1776, che «il totale rigetto delle soluzioni automatizzate che da tempo sono impiegate in altri ordinamenti non eviterà che presto si inizino ad apprezzare gli innegabili aspetti di efficienza e rapidità propri degli strumenti di IA, e di certo non metterà al riparo il nostro processo dai rischi connaturati nei modelli computazionali».

principi e regole – anche etiche – previsti dal diritto positivo o connaturali alla stessa natura umana, necessitano ora di essere espressamente riconosciuti, affermati e disciplinati. Il giurista[49] deve pertanto «procedere a tematizzare tali implicazioni, cominciare a riflettere su di esse e prospettare questioni e soluzioni, al fine di non aggravare il ritardo del diritto […] di fronte all'evoluzione tecnologica»[50].

Davanti a questa irruzione del progresso[51], tutta una serie di quesiti circa le correlazioni tra IA e diritto in genere è già stata individuata dal Parlamento Europeo nei *Considerando* della Risoluzione sopra menzionata, ove si afferma che:

> «B. […] l'umanità si trova ora sulla soglia di un'era nella quale *robot*, bot, androidi e altre manifestazioni dell'intelligenza artificiale sembrano sul punto di avviare una nuova rivoluzione industriale, suscettibile di toccare tutti gli strati sociali, rendendo imprescindibile che la legislazione ne consideri le implicazioni e le conseguenze legali ed etiche, senza ostacolare l'innovazione;
>
> G. […] l'andamento attuale, che tende a sviluppare macchine autonome e intelligenti, in grado di apprendere e prendere decisioni in modo indipendente, genera nel lungo periodo non solo vantaggi economici ma anche una serie di preoccupazioni circa gli effetti diretti e indiretti sulla società nel suo complesso;
>
> H. […] l'apprendimento automatico offre enormi vantaggi economici e innovativi per la società migliorando notevolmente le capacità di analisi dei dati, sebbene ponga nel contempo alcune sfide legate alla necessità di garantire la non discriminazione, il giusto processo, la trasparenza e la comprensibilità dei processi decisionali;
>
> O. […] gli sviluppi nel campo della robotica e dell'intelligenza artificiale possono e dovrebbero essere pensati in modo tale da preservare la dignità, l'autonomia e l'autodeterminazione degli individui […];
>
> Q. […] l'ulteriore sviluppo e il maggiore ricorso a processi decisionali automatizzati e algoritmici hanno senza dubbio un impatto sulle scelte compiute da un privato (ad esempio un'impresa o un internauta) e da un'autorità amministrativa, giudiziaria o da un qualsiasi

[49] Le nuove tecnologie si sono radicate nel quotidiano anche del giurista, il quale «da giurista umanista tende ad assumere le vesti di "giurista tecnologico"» per studiarne gli effetti. Così, S. SIGNORATO, *Le indagini digitali*, op. cit., p. 11.

[50] Così, F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 3. Analogamente, M. BASSINI – L. LIGUORI – O. POLLICINO, *Sistemi di Intelligenza Artificiale,* op. cit., p. 334, si osserva che nel passaggio dalla "società dell'informazione" basata su Internet alla "società dell'algoritmo", «I problemi che si pongono per il giurista sono analoghi a quelli che hanno contraddistinto altre "transazioni" tecnologiche: verificare l'idoneità delle norme esistenti ad applicarsi alle nuove tecnologie, così da valutare se sia opportuno, per i legislatori, coniare delle regole *ad hoc*, nuove, ovvero persistere, non senza possibili forzature avallate, magari, sul piano giurisprudenziale, nell'applicazione delle norme preesistenti».

[51] Rileva G.F. ITALIANO, *Intelligenza artificiale, che errore lasciarla agli informatici*, op. cit., penultimo capoverso, che «il progresso irrompe, non chiede permesso».

altro ente pubblico al fine di rappresentare la decisione finale di un consumatore, un'impresa o un'autorità; […] i dispositivi di sicurezza e la possibilità di verifica e controllo umani devono essere integrati nei processi decisionali automatizzati e algoritmici»[52].

Notevoli passi sono stati fatti negli ultimi anni nell'ambito dell'Unione europea e del Consiglio d'Europa per riflettere sulle modalità con cui sviluppare sistemi di IA sicuri e rispettosi dei diritti fondamentali. Le considerazioni svolte in Unione europea non riguardano principalmente l'ambito giuridico, ma rientrano nella più generale strategia per l'IA che la Commissione europea ha presentato nell'aprile 2018[53] nell'ottica di recuperare il ritardo sul tema rispetto agli operatori internazionali americani ed asiatici ed i cui obiettivi sono: aumentare gli investimenti pubblici e privati portandoli ad almeno 20 miliardi di euro l'anno nei prossimi dieci anni, mettere a disposizione più dati, promuovere il talento e garantire la fiducia[54]. Invece, nel contesto del Consiglio d'Europa sono stati fatti degli approfondimenti relativi al rapporto tra IA e sistemi giudiziari[55], non mancando tuttavia di affrontare anche le problematiche insite nel generale utilizzo dell'intelligenza artificiale[56]. Gli strumenti di IA giuridica disponibili sono infatti di vari tipi, dotati

[52] Così, Risoluzione del Parlamento Europeo del 16 febbraio 2017, cit., Considerando indicati.

[53] Commissione europea, *L'intelligenza artificiale per l'Europa*, COM(2018) 237 final, Brussels, 25.4.2018. La stessa Commissione ha pubblicato nel dicembre successivo il *Piano coordinato sull'intelligenza artificiale* (COM(2018) 795 final, Brussels, 7.12.2018), avviando una Alleanza europea per l'Intelligenza artificiale e istituendo un Gruppo di esperti di alto livello sull'IA, di cui si dirà subito dopo nel testo. Nel Piano coordinato tutti gli Stati Membri sono stati invitati a sviluppare le loro strategie nazionali per l'IA, delineando i livelli di investimento e le misure di attuazione. L'Italia ha provveduto in tal senso istituendo presso il Ministero dello Sviluppo Economico un gruppo di esperti che ha elaborato delle proposte, sintetizzate poi dal Ministero stesso nel luglio 2019 nella *Strategia nazionale per l'intelligenza artificiale* (reperibile *online* al collegamento https://www.mise.gov.it/images/stories/documenti/Strategia-Nazionale-Intelligenza-Artificiale-Bozza-Consultazione.pdf, consultato da ultimo in data 21 giugno 2022). Successivamente, la Commissione europea è nuovamente intervenuta pubblicando il *Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia* (COM(2020) 65 final, Brussels, 19.2.2020) per delineare un sistema europeo di eccellenza e fiducia per l'IA (reperibile *online* al collegamento https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_it.pdf, consultato da ultimo in data 21 giugno 2022) e la Comunicazione *Promuovere un approccio europeo all'intelligenza artificiale* (COM(2021) 205 final, Brussels, 21.4.2021) per presentare una proposta di quadro normativo sull'IA ed un piano coordinato riveduto sull'IA (reperibile *online* al collegamento https://data.consilium.europa.eu/doc/document/ST-8334-2021-INIT/it/pdf, consultato da ultimo in data 21 giugno 2022).

[54] Il percorso sull'intelligenza artificiale è iniziato sostanzialmente con la comunicazione della Commissione, del 13 settembre 2017, dal titolo "*Investire in un'industria intelligente, innovativa e sostenibile*", che sottolineava come l'intelligenza artificiale sia uno degli strumenti per portare l'industria a un livello adeguato all'era digitale, a cui sono poi seguite varie conclusioni adottate dal Consiglio Europeo e la definizione di piani sullo sviluppo ed utilizzo dell'intelligenza artificiale.

[55] CEPEJ – Gruppo di lavoro sulla qualità della Giustizia (CEPEJ-GT-QUAL), *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, 2019 (reperibile *online* al collegamento https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348, consultato da ultimo in data 21 giugno 2022).

[56] Nel maggio 2019, il Commissariato per i Diritti Umani del Consiglio d'Europa ha indicato nel documento *Unboxing Artificial Intelligence: 10 steps to protect Human Rights* alcune raccomandazioni per prevenire l'impatto negativo dovuto dall'utilizzo di applicativi di IA sui diritti fondamentali degli individui (reperibile *online* al collegamento https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64, consultato da ultimo in data 21 giugno 2022). Con lo scopo di predisporre un quadro giuridico per lo sviluppo, la progettazione e l'applicazione dell'IA basata sugli standard del Consiglio d'Europa in materia di diritti umani, democrazia e stato di diritto è stato istituito sempre nel 2019 il Comitato *ad hoc* per l'intelligenza artificiale (CAHAI), che l'anno successivo ha adottato uno studio di fattibilità in tal senso. Cfr. CAHAI, *Feasibility Study*, 17 dicembre 2020

di caratteristiche, finalità ed ambiti di impiego estremamente variegati: si tratta di sistemi di ricerca giurisprudenziale, strumenti di risoluzione delle controversie (*Online Dispute Resolution*), dispositivi di polizia predittiva, terminali di assistenza legale, strumenti di ausilio alla decisione ed apparati volti alla previsione della recidiva (*risk assessment tools*).

Coniugando lo sviluppo tecnologico con il rispetto dei diritti fondamentali, l'Europa potrebbe riacquistare un ruolo di centralità nella scena politica mondiale, ritagliandosi un ruolo chiave tra i sistemi americano ed asiatico, ove, per diversi motivi culturali e politici, il primato – a questo punto, ancóra universale o solo relativo? – dei diritti umani viene svilito a favore di interessi economici e di sistema[57].

Con il fine di affrontare le summenzionate problematiche, spingere aziende e ricercatori a sviluppare l'intelligenza artificiale in modo etico e trasparente, favorire un utilizzo corretto dei nuovi sistemi da parte degli addetti ai lavori e generare fiducia da parte dei cittadini-utenti quali oggetti attivi e passivi dell'attività degli applicativi, l'8 aprile 2019[58] il citato Gruppo Indipendente composto da 52 esperti sull'intelligenza artificiale nominato l'anno prima dalla Commissione europea ha pubblicato il documento *Orientamenti etici per un'IA affidabile*[59] con cui ha predisposto delle linee guida[60] concrete per realizzare una «IA affidabile basata sui diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea e dal pertinente diritto internazionale in materia di diritti umani»[61]. Anche se non riguardanti in particolare i sistemi utilizzati in ambito giuridico[62], le linee guida cercano di superare problematiche quali le discriminazioni che potrebbero

---

(reperibile *online* al collegamento https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da, consultato da ultimo in data 21 giugno 2022). Sullo studio di fattibilità, si veda C. BARBARO, *Lo studio di fattibilità di un nuovo quadro normativo sulla concezione, lo sviluppo e l'applicazione dei sistemi di Intelligenza Artificiale sulla base delle norme del Consiglio d'Europa. Il lavoro del Comitato Ad hoc sull'intelligenza artificiale del Consiglio d'Europa (CAHAI)*, in www.questionegiustizia.it, 28 aprile 2021 (reperibile *online* al collegamento https://www.questionegiustizia.it/data/doc/2879/barbaro-studio-di-fattibilita.pdf, consultato da ultimo in data 21 giugno 2022).

[57] Cfr. Commissione europea, Comunicazione *Promuovere un approccio europeo*, op. cit., p. 11.

[58] Lo stesso giorno la Commissione europea con la terza Comunicazione sull'IA (COM(2019) 168 final, Brussels, 8.4.2019) avvallava il contenuto del lavoro svolto e passava alla successiva fase del progetto sull'intelligenza artificiale consistente nell'attuazione e valutazione nella pratica degli orientamenti indicati (reperibile *online* al collegamento https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2019)168&lang=it, consultato da ultimo in data 21 giugno 2022).

[59] Gruppo Indipendente di esperti ad alto livello sull'intelligenza artificiale, *Orientamenti etici per un'IA affidabile*, 8 aprile 2019 (reperibile *online* al collegamento https://op.europa.eu/it/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1, consultato da ultimo in data 21 giugno 2022). Titolo originale dell'opera: *Ethics Guidelines for Trustworthy AI*.

[60] Per un'analisi approfondita delle linee guida, si veda N.A. SMUHA, *The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence*, in *Computer Law Review International*, vol. 20, n. 4/2019, pp. 97-106 (reperibile *online* al collegamento https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3443537, consultato da ultimo in data 21 giugno 2022). Nathalie A. Smuha era coordinatrice del Gruppo di esperti ad alto livello sull'IA.

[61] Gruppo Indipendente, *Orientamenti etici per un'IA affidabile*, op. cit., p. 7.

[62] Infatti, le Linee guida formulate dal Gruppo di esperti sull'IA «*are meant to apply to all AI systems*» (tradotto: «sono pensate per l'applicazione su tutti i sistemi di IA»). Così, N.A. SMUHA, *The EU Approach to Ethics*, op. cit., p. 16.

derivare da distorsioni di valutazione causate da pregiudizio (*bias*)[63] contenute nei programmi, l'opacità dei processi computazionali e il possibile condizionamento del risultato algoritmico sulla decisione umana, in modo da permettere l'impiego di dispositivi di IA nelle politiche pubbliche. Infatti, per fare in modo che l'IA sia «un mezzo promettente per aumentare la prosperità umana», è necessario che siano realizzati sistemi di IA «antropocentrici»[64], che garantiscano la «centralità dell'essere umano nel rapporto con l'Intelligenza Artificiale: prima devono venire la dignità e la libertà umane, anche e soprattutto quando entrano in gioco gli algoritmi. L'autonomia delle persone deve sempre prevalere sull'autonomia artificiale, pertanto deve essere garantito un potere di supervisione da parte degli uomini sulle macchine, in modo da limitare le decisioni di queste ultime»[65].

La Carta etica non è il primo lavoro di questo tipo[66]: infatti, simili iniziative erano già state intraprese sia da Paesi europei che extra-europei nel contesto delle loro strategie nazionali[67] sia, a livello internazionale, da organizzazioni governative[68] e non[69]. La Commissione europea ha però

---

[63] Per una breve analisi di come un dispositivo di IA possa dare un risultato influenzato da pregiudizio, si veda K. HAMMOND, *5 unexpected sources of bias in artificial intelligence*, in www.techcrunch.com, 10 dicembre 2016 (disponibile *online* al collegamento https://techcrunch.com/2016/12/10/5-unexpected-sources-of-bias-in-artificial-intelligence/?guccounter=2, consultato da ultimo in data 21 giugno 2022).

[64] Gruppo Indipendente, *Orientamenti etici per un'IA affidabile*, op. cit., p. 5.

[65] In questi termini, L. BOLOGNINI, *Codice etico UE sull'intelligenza artificiale: forte la tecnica, debole la politica*, in www.focus.it, 2 gennaio 2019 (reperibile *online* al collegamento https://www.focus.it/tecnologia/digital-life/commissione-europea-e-intelligenza-artificiale, consultato da ultimo in data 21 giugno 2022).

[66] Cfr. N.A. SMUHA, *The EU Approach to Ethics Guidelines*, op. cit., pp. 16-17.

[67] Si riportano, per esempio, la relazione *AI in the UK: ready, willing and able?*, pubblicata nel 2018 dal Comitato sull'intelligenza artificiale della House of Lords (reperibile *online* al collegamento https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf, consultato da ultimo in data 21 giugno 2022), che al paragrafo 417, a p. 125, intitolato "*Five overarching principles for an AI code*", indica una serie di principi sull'IA; *For a Meaningful Artificial Intelligence*, pubblicato nel 2018 dal matematico e membro dell'Assemblea Nazionale Francese Cédric Villani quale parte di una missione conferitagli dal Primo Ministro della Repubblica Francese (reperibile *online* al collegamento https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf, consultato da ultimo in data 21 giugno 2022).

[68] Nel contesto dell'Unione europea, si veda il lavoro del Gruppo Europeo per l'Etica delle Scienze e delle Nuove Tecnologie, *Statement on artificial intelligence, robotics and "autonomous" systems*, 9 marzo 2018 (reperibile *online* al collegamento https://op.europa.eu/it/publication-detail/-/publication/dfebe62e-4ce9-11e8-be1d-01aa75ed71a1, consultato da ultimo in data 21 giugno 2022).

[69] Per esempio, tra i contributi più significativi si possono menzionare: *Asilomar AI Principles*, stilato nel 2017 sotto gli auspici dell'Istituto Future of Life (reperibile *online* al collegamento https://futureoflife.org/ai-principles/?cn-reloaded=1, consultato da ultimo in data 21 giugno 2022); *Montréal Declaration for a Responsible Development of Artificial Intelligence*, a cura dell'Università di Montréal, 2018 (reperibile *online* al collegamento https://www.montrealdeclaration-responsibleai.com/the-declaration, consultato da ultimo in data 21 giugno 2022); capitolo "*General Principles*" della seconda versione del testo *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*, pp. 20-32, pubblicato nel 2018 dall'organizzazione IEEE (Insitute of Elettrical and Electronic Engeneers) (reperibile *online* al collegamento https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v2.pdf, consultato da ultimo in data 21 giugno 2022); *AI4People – An Ethical Framework for a Good IA Society: Opportunities, Risks, Principles, and Recommendations*, lavoro svolto nel 2018 dal Gruppo di AI4People (reperibile *online* al collegamento https://link.springer.com/article/10.1007/s11023-018-9482-5#Sec8, consultato da ultimo in data 21 giugno 2022; vedi nota oltre per indicazioni bibliografiche più dettagliate sul lavoro del Gruppo di AI4People); D.F. ENGSTROM – D.E. HO – C.M. SHARKEY – M.F. CUÉLLAR (a cura di), *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies. Report submitted to the Administrative Conference of the United States*, 2020 (reperibile

voluto incaricare un Gruppo di esperti ad alto livello sull'IA di fornire delle indicazioni e regole comuni sovranazionali ai vari attori che operano nel Mercato unico europeo[70]; tra l'altro, proprio nel solco tracciato dalla Carta etica sono seguiti altri lavori a livello nazionale[71] ed internazionale[72].

La Carta etica, procedendo nei tre capitoli che la compongono sulla linea astrazione-concretezza[73], ha il pregio di fornire numerose indicazioni tecniche utili all'applicazione pratica dei principi fondamentali del diritto europeo nello sviluppo di sistemi intelligenti, ma ha il limite di non contenere norme vincolanti sul piano giuridico[74]. La sua applicazione è quindi rimessa ai singoli governi, ai ricercatori e alle imprese. Nel terzo capitolo fornisce addirittura una lista di controllo concreta e flessibile allo specifico caso d'uso del sistema di IA, adatta a valutare l'operatività dei requisiti enunciati nel secondo capitolo e a verificare l'aderenza dell'IA stessa alle raccomandazioni etiche della Commissione europea nelle fasi di progettazione ("*by design*"), distribuzione ed utilizzo.

Durante l'intero ciclo di vita, il sistema di IA, per essere ritenuto affidabile, deve basarsi su tre componenti: legalità, eticità e robustezza.

Per quanto riguarda la legalità, l'IA deve ottemperare a tutte le disposizioni normative pertinenti, quali il diritto primario dell'UE (i Trattati dell'Unione e la Carta dei diritti fondamentali dell'Unione europea[75]), il diritto derivato dell'UE (ad esempio, il regolamento sulla protezione dati e la direttiva macchine), i trattati ONU sui diritti umani, le convenzioni del Consiglio d'Europa (su tutte, la Convenzione europea dei diritti dell'uomo), le norme degli Stati Membri dell'UE e le specifiche norme di settore nel quale il dispositivo è applicato. «I trattati dell'UE e la Carta dell'UE

---

online al collegamento https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf, consultato da ultimo in data 21 giugno 2022). Quest'ultimo studio, frutto del lavoro di giuristi, informatici e studiosi di scienze sociali delle Università di Stanford e di New York, presenta numerosi profili di interesse pratico e teorico per il dibattito giuridico sull'intelligenza artificiale. Per un commento sulla relazione, si veda L. PARONA, *"*Government by algorithm*": un contributo allo studio del ricorso all'intelligenza artificiale nell'esercizio di funzioni amministrative*, in *Giornale di diritto amministrativo*, n. 1/2021, pp. 10-18.

[70] Cfr., N.A. SMUHA*, The EU Approach to Ethics Guidelines*, op. cit., p. 4.

[71] Per il contesto italiano, si segnala il contributo *Statuto Etico e Giuridico dell'IA* elaborato nel 2019 dalla Fondazione Leonardo – Civiltà delle Macchine (reperibile *online* al collegamento https://www.civiltadellemacchine.it/it/la-fondazione/umanesimo-digitale/la-carta-etica-e-giuridica-dell-ia, consultato da ultimo in data 21 giugno 2022); lo Statuto dedica una specifica sezione ai principi giuridici (pp. 52 e ss.). Per un primo commento sulla specifica sezione giuridica, si veda C. MORELLI, *Intelligenza artificiale, ecco lo statuto giuridico*, in www.altalex.com, 9 dicembre 2019 (reperibile *online* al collegamento https://www.altalex.com/documents/news/2019/12/09/intelligenza-artificiale-statuto-giuridico, consultato da ultimo in data 21 giugno 2022).

[72] Si veda il lavoro *Principles on Artificial Intelligence* dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) del maggio 2019 (reperibile *online* al collegamento https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, consultato da ultimo in data 21 giugno 2022).

[73] Cfr. Gruppo Indipendente, *Orientamenti etici per un'IA affidabile*, op. cit., p. 8.

[74] Si precisa infatti che «Nulla di quanto contenuto nel presente documento crea diritti giuridici o impone obblighi giuridici nei confronti di terzi». *Idem*, Punto 25, p. 8.

[75] L'Unione europea si fonda su un impegno costituzionale a tutelare i diritti fondamentali e indivisibili degli esseri umani, a garantire il rispetto dello Stato di diritto, a promuovere la libertà democratica e il bene comune. Questi diritti sono sanciti negli articoli 2 e 3 del Trattato sull'Unione europea e nella Carta dei diritti fondamentali dell'Unione europea (cd. Carta di Nizza).

sanciscono una serie di diritti fondamentali che gli Stati membri e le istituzioni dell'UE sono giuridicamente tenuti a rispettare quando attuano il diritto unionale[76]. Tali diritti sono descritti nella Carta dei diritti fondamentali dell'Unione europea con riferimento alla dignità, alle libertà [individuali], all'uguaglianza [, non discriminazione e] solidarietà, ai diritti dei cittadini e al [rispetto della democrazia, della] giustizia [e dello Stato di diritto][77]. Il fondamento che accomuna questi diritti può essere inteso come radicato nel rispetto della dignità umana e della libertà individuale, riflettendo così […] un "approccio antropocentrico" in cui l'essere umano gode di uno *status* morale unico e inalienabile di primato in campo civile, politico, economico e sociale»[78].
Con "dignità umana" si fa appunto riferimento a quel concetto per cui ogni essere umano ha un proprio valore intrinseco, che non deve essere influenzato o danneggiato né dagli altri uomini, né dalle IA: per i primi, la dignità umana funge da limite per le azioni e l'autodeterminazione proprie ed altrui; per le seconde, «il rispetto per la dignità umana implica che tutte le persone siano trattate con il rispetto loro dovuto in quanto *soggetti* morali, piuttosto che come semplici *oggetti* da vagliare, catalogare, valutare per punteggio, aggregare, condizionare o manipolare»[79].

Invece, per quanto riguarda la libertà individuale, l'essere umano deve poter prendere liberamente decisioni importanti per sé stesso. «Nell'ambito dell'IA, per salvaguardare la libertà individuale occorre ridurre al minimo la coercizione illegittima diretta o indiretta, le minacce all'autonomia mentale e alla salute psichica, la sorveglianza ingiustificata, l'inganno e la manipolazione iniqua»[80]. All'interno del concetto di libertà individuale assume poi particolare importanza la *privacy*, che si scontra con la necessità fisiologica dei dispositivi di IA di avere a disposizione grandi quantità di dati al momento della progettazione e nella successiva fase di apprendimento automatico per funzionare. Per trovare un punto di equilibrio tra la *privacy* dei dati e la necessità delle macchine di poter attingere a quei dati, l'essere umano deve essere posto nella

[76] A norma dell'articolo 51, le disposizioni della Carta si applicano alle istituzioni dell'Unione come pure agli Stati membri nell'attuazione del diritto dell'Unione.

[77] Rileva il Gruppo Indipendente, *Orientamenti etici per un'IA affidabile*, op. cit., Punto 40, p. 11, che nei lavori che intendono delineare un quadro etico per l'IA vi è una generale concordanza su queste «famiglie di diritti fondamentali […] particolarmente pertinenti per quanto riguarda i sistemi di IA»; tali famiglie sono riassunte nel lavoro cit. *Asilomar AI Principles* al Principio n. 11: «*Human Values*: *AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity*».

[78] Così, Gruppo Indipendente, *Orientamenti etici per un'IA affidabile*, op. cit., Punto 38, p. 11. Riformulazione secondo capoverso mia, cfr. *Idem*, p. 12.

[79] *Idem*, Punto 41, p. 12. Allo stesso modo, la Fondazione Leonardo, *Statuto Etico*, op. cit., pp. 31-32, sottolinea come sembrino «[c]ontrarie alla dignità umana [quelle] tecnologie che manipolano l'utente – anche a fine di bene – o a cui sono delegate decisioni di grande importanza sociale o esistenziale senza che sia possibile comprenderne le dinamiche» e che «non colgono il valore intrinseco di ogni individuo dissolvendo la sua particolarità nella generalità di modelli statistici».

[80] Così, Gruppo Indipendente, *Orientamenti etici per un'IA affidabile*, op. cit., Punto 42, p. 12. Similmente, l'Università di Montréal, *Montréal Declaration for a Responsible AI*, op. cit., Principio 3.3, afferma che sistemi di IA «*must not be developed or used to impose a particular lifestyle on individuals, whether directly or indirectly, by implementing oppressive surveillance and evaluation or incentive mechanisms*» (tradotto: «non devono essere sviluppati o utilizzati per imporre agli individui, direttamente o indirettamente, un particolare stile di vita attraverso l'attuazione di sorveglianza oppressiva o meccanismi di valutazione ed incentivazione»).

condizione di poter sempre sapere quali e quanti dei suoi dati personali vengono raccolti, per quali fini verranno usati e poterne richiedere l'eliminazione[81].

Invece, per garantire eticità e robustezza, è necessario tradurre i principi fondamentali in principi etici. Allo stesso modo, gli individui e la società devono essere sicuri che i sistemi di IA funzionino in modo sicuro e affidabile, non causando alcun danno involontario. Dovrebbero quindi essere previste misure di salvaguardia per prevenire qualsiasi effetto negativo indesiderato. I sistemi di IA dunque devono essere robusti sia da un punto di vista tecnico (garantendo la robustezza tecnica del sistema in un dato contesto, ad esempio il settore di applicazione o la fase del ciclo di vita), sia da un punto di vista sociale (tenendo in debita considerazione il contesto e l'ambiente in cui il sistema opera). L'eticità e la robustezza dell'IA sono quindi componenti strettamente correlate che si integrano a vicenda.

Nell'Unione europea, il Gruppo europeo per l'etica delle scienze e delle nuove tecnologie (EGE)[82], traendo ispirazione dai diritti fondamentali per produrre un quadro etico per l'IA, aveva già proposto una serie di 9 principi, basati sui valori fondamentali sanciti dai Trattati e dalla Carta dei diritti fondamentali dell'Unione europea[83]. A sua volta, la Carta etica, basandosi sul lavoro fatto, elenca quattro principi ai quali occorre aderire per garantire che i sistemi di IA siano sviluppati, distribuiti e utilizzati in modo affidabile. Gli «imperativi etici», sono i seguenti: 1) rispetto dell'autonomia umana; 2) prevenzione dei danni; 3) equità; 4) esplicabilità.

L'elencazione non è legata ad una questione gerarchica, ma segue l'ordine di apparizione dei diritti fondamentali su cui gli imperativi si basano all'interno della Carta dei diritti fondamentali dell'Unione europea: infatti, il rispetto dell'autonomia umana è strettamente connesso al diritto alla dignità umana e alla libertà (sanciti dagli artt. 1 e 6 della Carta); la prevenzione dei danni è riferita alla protezione dell'integrità fisica e psichica (affermata dall'articolo 3); l'equità è strettamente connessa ai diritti alla non discriminazione, alla solidarietà e alla giustizia (artt. 21 e ss.); infine, l'esplicabilità e la responsabilità sono strettamente connesse ai diritti relativi alla giustizia (sanciti dall'articolo 47).

---

[81] Cfr. Future of Life Institute, *Asilomar AI Principles*, cit., Principi n. 12 e 13.

[82] European Groups on Ethics (EGE).

[83] Si tratta dei principi di: dignità umana; autonomia; responsabilità; giustizia, equità e solidarietà; democrazia; stato di diritto ed esplicabilità (*accountability*); sicurezza (*security*), incolumità (*safety*) ed integrità fisica e mentale. Gruppo Europeo per l'Etica delle Scienze e delle Nuove Tecnologie, *Statement on artificial intelligence*, cit., pp. 16-19. Successivamente, il Gruppo di AI4People ha esaminato i summenzionati principi del Gruppo Europeo per l'Etica delle Scienze e delle Nuove Tecnologie più altri 36 principi etici presentati fino a quel momento da altre organizzazioni pubbliche e private e li ha classificati in cinque grandi categorie: beneficialità (*beneficence*); non maleficenza (*non-maleficence*); autonomia [di decisione]; giustizia; esplicabilità. L. FLORIDI – J. COWLS – M. BELTRAMETTI – R. CHATILA – P. CHAZERAND – V. DIGNUM – C. LUETGE – R. MADELIN – U. PAGALLO – F. ROSSI – B. SCHAFER – P. VALCKE – E.J.M. VAYENA, *AI4People – An Ethical Framework for a Good IA Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, n. 28(4), 2018, pp. 689-707 (reperibile *online* al collegamento https://link.springer.com/article/10.1007/s11023-018-9482-5#Sec8, consultato da ultimo in data 21 giugno 2022).

Circa il rispetto dell'autonomia umana, gli esseri umani che interagiscono con i sistemi di IA devono poter mantenere la propria piena ed effettiva autodeterminazione, non essendo in alcun modo subordinati o condizionati dall'applicativo; garantendo la sorveglianza ed il controllo dei processi operativi, si riesce, appunto, ad impostare un sistema di IA antropocentrico.

Per prevenzione dei danni si intende la necessità di tutelare la dignità e l'integrità fisica e psichica dell'uomo, evitando che l'applicativo di IA causi danni o li aggravi. I sistemi di IA e gli ambienti in cui operano devono essere sicuri e protetti; inoltre, come già anticipato, devono essere tecnicamente robusti e non possono essere utilizzati per scopi malevoli.

L'attività del sistema di IA deve anche essere caratterizzata da equità sostanziale e procedurale. Per il piano sostanziale, è necessario che l'attività stessa eviti di tradursi in discriminazioni e distorsioni, rispetti il principio di proporzionalità tra mezzi e fini[84] e valuti come bilanciare interessi concorrenti. Di conseguenza, le misure adottate per raggiungere un obiettivo dovrebbero essere limitate allo stretto necessario, preferendo le modalità meno lesive dei diritti fondamentali e delle norme etiche. Invece, l'affermazione dell'equità sul piano procedurale comporta la possibilità per gli esseri umani destinatari delle decisioni elaborate dai sistemi di IA di impugnarle e presentare ricorso contro di esse, avendo chiaro chi è la figura o l'organismo responsabile della decisione e potendo ottenere spiegazione della motivazione che sta alla base della decisione stessa.

Infine, l'«esplicabilità è fondamentale per creare e mantenere la fiducia degli utenti nei sistemi di IA. Tale principio implica che i processi devono essere trasparenti, le capacità e lo scopo dei sistemi di IA devono essere comunicati apertamente e le decisioni, per quanto possibile, devono poter essere spiegate a coloro che ne sono direttamente o indirettamente interessati. Senza tali informazioni, una decisione non può essere debitamente impugnata. Non sempre è possibile spiegare, tuttavia, perché un modello ha generato un particolare risultato o decisione (e quale combinazione di fattori di *input* vi ha contribuito). È il cosiddetto caso della "scatola nera" i cui algoritmi richiedono un'attenzione particolare. In tali circostanze, possono essere necessarie altre misure per garantire l'esplicabilità (ad esempio, la tracciabilità, la verificabilità e la comunicazione trasparente sulle capacità del sistema), posto che il sistema nel suo complesso rispetti i diritti fondamentali. Il grado di esplicabilità necessario dipende in larga misura dal contesto e dalla gravità delle conseguenze nel caso in cui il risultato sia errato o comunque impreciso»[85].

Per ottenere un'IA affidabile, i tre principi astratti delineati nel I capitolo devono essere tradotti in requisiti concreti, che il sistema di IA dovrebbe soddisfare grazie all'attuazione di metodi

[84] È possibile far riferimento anche alla proporzionalità tra utente e distributore, considerando i diritti delle imprese (compresa la proprietà intellettuale e la riservatezza), da un lato, e i diritti dell'utente, dall'altro.

[85] Così, Gruppo Indipendente, *Orientamenti etici per un'IA affidabile*, op. cit., Punto 53, pp. 14-15.

tecnici e non tecnici[86]; i requisiti individuati dalla Carta sono: 1) intervento e sorveglianza umani, 2) robustezza tecnica e sicurezza, 3) riservatezza e gestione (*governance*) dei dati, 4) trasparenza, 5) diversità, non discriminazione ed equità, 6) benessere sociale e ambientale e 7) responsabilità e rendere conto (*accountability*)[87].

Nell'attuazione di questi requisiti, potrebbero sorgere delle frizioni tra loro e non sempre il compromesso è accettabile. «Nelle situazioni in cui non possibile trovare compromessi eticamente accettabili, lo sviluppo, la distribuzione e l'utilizzo del sistema di IA non dovrebbero procedere secondo quel modello. Qualunque decisione sul compromesso da accettare deve essere motivata e adeguatamente documentata. Il decisore deve assumersi la responsabilità delle modalità di attuazione del compromesso più adeguato e deve riesaminare costantemente l'adeguatezza della decisione che ne deriva per garantire che possano essere apportate le necessarie modifiche al sistema ove opportuno»[88].

I sistemi di IA dovrebbero sostenere l'autonomia e il processo decisionale umani, come prescrive l'imperativo etico del rispetto dell'autonomia umana; in tal senso, l'art. 22, co. 1 del Regolamento (UE) n. 2016/679 sulla protezione dei dati (GDPR) ha già sancito «[per] [l]'interessato […] il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato […] che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». La sorveglianza umana, da attuare con approccio più o meno incisivo[89], è ulteriore elemento volto ad evitare che l'IA pregiudichi l'autonomia umana o produca effetti capaci di influenzare negativamente la decisione autonoma ed informata dell'utente.

Tracciabilità dei dati e dei processi utilizzati dall'IA per svolgere la propria funzione e spiegabilità delle decisioni sono invece volte a garantire il requisito della trasparenza.

Infine, per assicurare la fiducia degli utenti, è necessario poter verificare e valutare

[86] Cfr. *Idem*, pp. 23-28. Per esempio, per verificare ed approvare l'elaborazione dei dati, tra i metodi tecnici si fa rientrare il monitoraggio della macchina attraverso continue attività di prova e convalida, mentre tra i metodi non tecnici sono previste la dotazione di codici di condotta interni ai portatori di interesse (organizzazioni, aziende, ecc.) e la possibilità di ricorrere a organizzazioni indipendenti che possano certificare per il pubblico generale che un sistema di IA è trasparente, responsabile ed equo.

[87] Requisito che può anche tradursi più semplicemente col termine "responsabilizzazione".

[88] *Idem*, Punto 90, p. 23.

[89] Cfr. *Idem*, Punto 65, p. 18: «L'approccio [con intervento umano (*human-in-the-loop* – HITL)] prevede la possibilità di intervento umano in ogni ciclo decisionale del sistema, che in molti casi non è né possibile[,] né auspicabile. L'approccio [con supervisione umana (*human-on-the-loop* – HOTL)] prevede l'intervento umano durante il ciclo di progettazione del sistema e il monitoraggio del funzionamento del sistema. L'approccio [basato sul controllo umano (*human-in-command* – HIC)] prevede il controllo dell'attività del sistema di IA nel suo complesso (compresi i suoi effetti generali a livello economico, sociale, giuridico ed etico) e la capacità di decidere quando e come utilizzare il sistema in qualsiasi particolare situazione. Si potrebbe anche decidere di non utilizzare un sistema di IA in una data situazione, di stabilire livelli di discrezionalità umana durante l'uso del sistema, o di garantire la capacità di ignorare una decisione presa da un sistema. Occorre inoltre garantire che le autorità pubbliche competenti abbiano la capacità di esercitare la sorveglianza in conformità al loro mandato. Potrebbero essere necessari meccanismi di sorveglianza a vari livelli a sostegno di altre misure di sicurezza e di controllo, a seconda del settore di applicazione del sistema di IA e del rischio potenziale. A parità di condizioni, minore è la sorveglianza che un essere umano può esercitare su un sistema di IA, maggiore è la necessità di prove esaurienti e di una *governance* rigorosa».

algoritmi, dati e processi di progettazione, prevedendo meccanismi di ricorso in caso di presunti effetti negativi ingiusti derivanti dalla decisione emessa. Nei casi in cui le applicazioni influiscano sui diritti fondamentali, occorre anche che il sistema di IA possa essere sottoposto ad una verifica indipendente.

1.3 IA e diritto: la *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*.

Sempre con l'intento di fornire dei principi per garantire un'IA etica e rispettosa dei diritti dei cittadini, ma con lo sguardo rivolto allo specifico ambito giudiziario, nel contesto del Consiglio d'Europa sono stati elaborati diversi lavori, volti ad esaminare fenomeni già esistenti e sperimentazioni in atto. Oltre alla diffusione di applicativi tecnologici basati o meno sull'IA (si pensi, ad esempio, in campo penale all'utilizzo, prima, di dispositivi per le intercettazioni ambientali e, ora, di più sofisticati captatori informatici), grazie all'enorme quantità di dati, messa a disposizione in appositi archivi digitali, ed agli sviluppi delle tecnologie di analisi linguistica, di *data mining* e di estrazione delle informazioni, si è imposta l'idea di poter governare algoritmicamente la giustizia, predisponendo degli strumenti di *machine learning* in grado di dare delle proiezioni future. A seconda della diversa tipologia dei dati inseriti nell'elaboratore (*input*), degli algoritmi di apprendimento utilizzati dal sistema (*learning algorithms*) e del risultato finale del procedimento di elaborazione (*output*), la tecnologia delle *machine learning* può operare nelle attività di analisi di documenti e predisposizione di atti, nell'ottica della c.d. giustizia predittiva[90] e della formulazione di giudizi.

A sua volta, nel campo della giustizia predittiva la modalità di utilizzo di un applicativo di IA può declinarsi in funzione di diverse finalità, cioè come dispositivo integrativo dell'attività del giurista per l'interpretazione della legge, per l'individuazione degli argomenti a favore della tesi che si intende sostenere e per la previsione dell'esito di un giudizio; strumento di prevenzione della criminalità (versante della giustizia preventiva) e strumento per calcolare la probabilità della

[90] Dato che gli algoritmi di *machine learning* costruiscono modelli elaborando dati storici, sarebbe più corretto parlare di "previsione", ossia di un'enunciazione compiuta in seguito ad un'osservazione (da *prae*, prima – *videre*, vedere), e non di "predizione", termine che secondo le radici latine (*praedire*: *prae*, prima – *dicere*, dire), indica l'atto di preannunciare il futuro in termini divinatori o profetici. Cfr. C. BARBARO, *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?*, in www.questionegiustizia.it, n. 4/2018, pp. 190-191 (reperibile *online* al collegamento https://www.questionegiustizia.it/rivista/2018-4.php, consultato da ultimo in data 21 giugno 2022); cfr. X. RONSIN – V. LAMPOS (a cura di), *Appendice I. Studio approfondito sull'utilizzo dell'IA nei sistemi giudiziari, segnatamente delle applicazioni dell'intelligenza artificiale rivolte al trattamento di decisioni e dati giudiziari*, in CEPEJ, *Carta etica europea*, cit., Punti 60-64, 146-153, pp. 23-24 e 38-40. Per una definizione di giustizia predittiva, nella stessa *Carta etica europea*, *Appendice III. Glossario*, p. 47.

recidiva (versante della giustizia preventivo-repressiva).

Infine, va rilevato come l'impiego di dispositivi di intelligenza artificiale non operi soltanto nel campo della predizione, ma anche nel campo della decisione, demandando al dispositivo il compito di affiancare o, addirittura, sostituire il giudice nell'emettere una decisione.

In questo contesto di plurime sperimentazioni, già nel 2018 veniva pubblicato lo studio dottrinale *Algorithms and Human Rights*[91], redatto dal Comitato di esperti sugli Intermediari Internet del Consiglio d'Europa, nella cui sezione *Fair trial and due process*[92] venivano esaminati i profili più critici degli strumenti di IA già in uso nel processo penale statunitense. Le principali preoccupazioni evidenziate dal Comitato attengono alla tenuta dei principi della presunzione di innocenza, della parità delle armi e del contraddittorio (sanciti dagli artt. 5, 6 e 7, Convenzione europea dei diritti dell'uomo), come anche al pericolo che i giudici impropriamente deleghino *tout court* la decisione a strumenti nati invece con il diverso fine di supportarli nella fase decisoria.

Cercando di rispondere a queste questioni e «calibrando e integrando alcuni dei principi generali [affermati nelle Linee guida commissionate dalla Commissione europea] rispetto alla realtà giudiziaria»[93], la Commissione europea per l'efficacia della giustizia (CEPEJ[94]) del Consiglio d'Europa, istituita nel 2002 per iniziativa del relativo Comitato dei Ministri, con lo scopo di monitorare e misurare la qualità dei sistemi giudiziari dei Paesi membri, ha stilato il 4 dicembre 2018 la *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*[95], che ad oggi può essere considerata il contributo più significativo in materia di IA e processo[96]. Oltre ad enunciare dei principi generali[97], la Carta etica è corredata da quattro

---

[91] Studio del Consiglio d'Europa, DGI (2017)12 – Committee of experts on Internet Intermediaries (MSI-NET), *Algorithms and Human Rights. Study on the Human Rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*, 2017 (reperibile *online* al collegamento https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5, consultato da ultimo in data 21 giugno 2022).

[92] *Idem*, pp. 10-12.

[93] In questi termini, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 61.

[94] Commission Européenne Pour l'Efficacité de la Justice – European Commission for the Efficiency of Justice.

[95] Per un primo commento ai contenuti della Carta, C. BARBARO (a cura di), *Cepej, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (IA) nei sistemi giudiziari*, in www.questionegiustizia.it, 7 dicembre 2018 (reperibile *online* al collegamento https://www.questionegiustizia.it/articolo/cepej-adottata-la-prima-carta-etica-europea-sull-uso-dell-intelligenza-artificiale-ai-nei-sistemi-giudiziari_07-12-2018.php, consultato da ultimo in data 21 giugno 2022).

[96] A fine 2019, in occasione della 33ª assemblea plenaria, la CEPEJ ha stabilito di formare un nuovo gruppo di lavoro per approfondire le riflessioni sul tema.

[97] Per l'analisi dei principi e delle relative problematiche a cui gli stessi devono porre rimedio, si vedano, *ex multis*, C. BARBARO, *Uso dell'intelligenza artificiale nei sistemi giudiziari*, op. cit., p. 195; S. QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in www.lalegislazionepenale.eu, 18 dicembre 2018 (reperibile *online* al collegamento http://www.lalegislazionepenale.eu/wp-content/uploads/2019/02/Carta-etica-LP-impaginato.pdf, consultato da ultimo in data 21 giugno 2022); A. TRAVERSI, *Intelligenza artificiale applicata alla giustizia: ci sarà un giudice* robot*?*, in www.questionegiustizia.it, 10 aprile 2019 (reperibile *online* al collegamento https://www.questionegiustizia.it/articolo/intelligenza-artificiale-applicata-alla-giustizia-ci-sara-un-giudice-robot-_10-04-2019.php, consultato da ultimo in data 21 giugno 2022); F. CERESA GASTALDO, *Lo statuto della giustizia digitale nella Carta etica della CEPEJ*, in www.iusinitinere.it, 2 aprile 2021 (reperibile *online* al collegamento

Appendici[98], di cui la prima contiene uno studio approfondito sull'utilizzo dell'IA nei sistemi giudiziari europei[99] e la seconda esamina i suoi diversi impieghi, incoraggiandone in diversa misura – cioè, attraverso questa gradazione: da incoraggiare; da utilizzare con alcune precauzioni; da rimandare a seguito di approfondimenti scientifici; da valutare con estrema cautela – l'applicazione in base alla compatibilità con i principi fissati[100].

Anche prima di questo risultato, la CEPEJ si era già interessata all'impatto delle tecnologie dell'informazione e della comunicazione sui sistemi giudiziari europei, redigendo nel biennio 2014-2016 il rapporto *Impiego delle tecnologie dell'informazione nei tribunali in Europa*[101] ed a fine 2016 le *Linee guida sulla cybergiustizia*[102], ove aveva mostrato apertura verso applicativi di IA che possono determinare un aumento dell'efficienza complessiva dei sistemi di giustizia, sollevando però al contempo perplessità circa l'impiego di programmi di analisi della giurisprudenza a supporto della decisione giudiziale. Se tra i benefici di un impiego virtuoso di tali strumenti si annoverano l'agevolazione dell'accesso alla giustizia, la semplificazione della comunicazione tra le corti e un generale miglioramento dell'organizzazione dei tribunali, il rischio maggiore è che un loro scorretto utilizzo possa creare una significativa minaccia alla capacità discrezionale ed all'indipendenza del giudice. Se allo stato è molto improbabile che gli strumenti a disposizione, di natura statistica, riescano a sostituire integralmente il giudice, è verosimile che possano comunque esercitare una significativa influenza sull'attività decisionale: infatti, come è stato evidenziato, «[è] facile immaginare che per chi decide possa diventare difficile discostarsi dal risultato di analisi elaborate da sofisticatissimi [programmi] in grado di processare migliaia di informazioni»[103].

La Carta etica stilata dalla CEPEJ, precedente agli *Orientamenti etici* elaborati dal Gruppo Indipendente in ambito UE, è il primo documento ad individuare delle linee guida fondamentali per l'utilizzo dell'IA a servizio dell'efficienza e qualità della giustizia ed a presentare un modello

---

https://www.iusinitinere.it/lo-statuto-della-giustizia-digitale-nella-carta-etica-della-cepej-36950, consultato da ultimo in data 21 giugno 2022).

[98] Per completezza, si segnala che la III Appendice reca un glossario, mentre la IV una lista di controllo di autovalutazione della compatibilità dei modelli di utilizzo con i principi enunciati dalla Carta.

[99] Cfr. X. RONSIN – V. LAMPOS (a cura di), *Appendice I*, cit., pp. 13-41.

[100] Cfr. CEPEJ, *Carta etica europea*, *Appendice II. Quali utilizzi dell'intelligenza artificiale nei sistemi giudiziari europei?*, pp. 42-44.

[101] CEPEJ, Studio n. 24, *Rapport thématique: l'utilisation des technologies de l'information par les tribunaux en Europe*, 2016 (dati del 2014) (reperibile *online* al collegamento https://rm.coe.int/systemes-judiciaires-europeens-efficacite-et-qualite-de-la-justice-etu/16807882c1, consultato da ultimo in data 21 giugno 2022).

[102] CEPEJ, *Guidelines on how to drive change towards cyberjustice. Stock-taking of tools deployed and summary of good practices*, 2016 (reperibile *online* al collegamento https://edoc.coe.int/fr/efficacite-de-la-justice/7501-guidelines-on-how-to-drive-change-towards-cyberjustice-stock-taking-of-tools-deployed-and-summary-of-good-practices.html, consultato da ultimo in data 21 giugno 2022).

[103] In questi termini, F. CERESA GASTALDO, *Il giudice-robot: l'intelligenza artificiale nei sistemi giudiziari tra aspettative ed equivoci*, in www.iusinitinere.it, 22 marzo 2021, p. 2 (reperibile *online* al collegamento https://www.iusinitinere.it/il-giudice-robot-lintelligenza-artificiale-nei-sistemi-giudiziari-tra-aspettative-ed-equivoci-36717#_ftn4, consultato da ultimo in data 21 giugno 2022).

formulato in articoli[104]. Anch'essa di natura non vincolante, quindi quale strumento di *soft law*, si rivolge «agli attori pubblici e privati incaricati di creare e lanciare strumenti e servizi di intelligenza artificiale relativi al trattamento di decisioni e dati giudiziari» ed ai «responsabili di decisioni pubbliche competenti in materia di quadro legislativo o regolamentare, o dello sviluppo, della verifica o dell'utilizzo di tali strumenti e servizi»[105]. Obiettivo della CEPEJ è quello di incoraggiare l'impiego di metodi computazionali per il rafforzamento della efficacia della giustizia, «nel dovuto rispetto dei diritti fondamentali della persona, enunciati nella Convenzione europea sui diritti dell'uomo e nella Convenzione per la protezione dei dati di carattere personale, e in conformità agli altri principi fondamentali [enunciati nella Carta]»[106].

I 5 principi generali affermati dalla Carta sono i seguenti: 1) rispetto dei diritti fondamentali; 2) non discriminazione; 3) qualità e sicurezza; 4) trasparenza, imparzialità ed equità; 5) garanzia del controllo da parte dell'utilizzatore.

Il primo principio (art. 1) vuole «assicurare che l'elaborazione e l'attuazione di strumenti e servizi di intelligenza artificiale siano compatibili con i diritti fondamentali»[107]. Tale formula non è «declamatoria»[108], in quanto il documento non si rivolge solamente agli Stati, ma anche agli operatori privati (dai produttori *software*, ai matematici, agli analisti), «comprensibilmente estranei all'articolato sistema delle garanzie fondamentali costruito all'interno del Consiglio d'Europa»[109], nella prospettiva di promuovere un'interazione tra scienze dure e scienze sociali per non lasciare la questione alle mere regole di domanda ed offerta del mercato.

Negli strumenti della Convenzione EDU e della Convenzione di Strasburgo n. 108/1981 per la protezione dei dati di carattere personale vanno individuate le garanzie per sviluppare e formare gli applicativi di IA fin dalla progettazione nel rispetto dei diritti umani (approccio etico fin dall'elaborazione o diritti umani fin dall'elaborazione[110]), qui declinati nei principi connessi all'amministrazione della giustizia, quali: il diritto di accesso alla giurisdizione; il diritto a un ricorso effettivo davanti a un giudice imparziale[111]; il diritto all'equo processo (*fair trial*), declinato nei principi di uguaglianza delle armi e di rispetto del contraddittorio; il principio di legalità;

[104] Cfr. S. QUATTROCOLO, *Intelligenza artificiale e giustizia*, op. cit., p. 4.
[105] CEPEJ, *Carta etica europea*, *Introduzione*, cit., p. 5.
[106] *Idem*, p. 5.
[107] *Idem*, p. 6.
[108] Così, S. QUATTROCOLO, *Intelligenza artificiale e giustizia*, op. cit., p. 4.
[109] *Eadem*, p. 4.
[110] Cfr. CEPEJ, *Carta etica europea*, cit., p. 7; l'approccio è definitivo anche *ethical-by-design* o *human-rights-by-design*.
[111] In questo senso, già l'art. 47 ("Diritto a un ricorso effettivo e a un giudice imparziale") della Carta dei diritti fondamentali dell'UE, riprendendo l'art. 13 della CEDU, stabilisce che: «Ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice […].
Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni persona ha la facoltà di farsi consigliare, difendere e rappresentare. […]».

l'indipendenza della magistratura e del giudice nell'esercizio del potere decisorio; il diritto di non discriminazione[112].

Perfino il più semplice ed innocuo strumento computazionale capace di attingere ai dati aperti (*open data*), cioè ai dati pubblici scaricabili, come tutte le sentenze pronunciate in un ordinamento, può «ingenerare effetti "di sistema", dall'impatto eclatante»[113]. In tema di indipendenza del giudice, un dispositivo non correttamente tarato potrebbe sia privilegiare la quantità delle pronunce giurisprudenziali a discapito della loro qualità, determinando così il rovesciamento del rapporto tra giurisdizioni inferiori e giurisdizioni superiori[114], alle quali spetta il ruolo di nomofilachia, sia causare una maggiore vincolatività del precedente, soprattutto negli ordinamenti di *Civil law* che non sono basati su di esso, imponendo addirittura un onere motivazionale rafforzato al giudice che se ne voglia discostare[115].

Il secondo principio, di non discriminazione (art. 2), è un corollario del principio di uguaglianza ed è volto a «prevenire specificamente lo sviluppo o l'intensificazione di discriminazioni tra persone o gruppi di persone»[116]. Il punto è che i dispositivi di IA possono dare risultati influenzati da pregiudizi, se i dati sui quale operano sono spuri, e particolare attenzione deve essere posta quando il trattamento è direttamente o indirettamente basato su dati "sensibili", quali origini razziali o etniche, origini socioeconomiche, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici, dati sanitari o dati relativi alla vita o all'orientamento sessuale. Per evitare tale pericolo, soprattutto in ambito penale, ove sono in gioco direttamente le libertà personali dell'interessato, gli attori pubblici e gli addetti ai lavori devono vigilare sull'effettiva efficacia dei dispositivi ed avere un ruolo propositivo nel loro sviluppo[117]. Così, quando in un sistema di AI viene identificato un processo che conduce di fatto ad una discriminazione, debbono essere adottate misure correttive per neutralizzare questi rischi unitamente alla sensibilizzazione dei soggetti coinvolti.

Il terzo principio (art. 3) fa riferimento ai concetti di qualità e sicurezza**,** applicabili in particolare nel delicato campo del trattamento dei dati relativi alle decisioni giudiziarie. La Carta etica osserva che è necessario, da un lato, che la macchina utilizzi fonti certificate e, dall'altro, che i

[112] Analogamente, l'OCSE, *Principles on Artificial Intelligence*, cit., Punto 1.2.a, p. 7, raccomanda il rispetto in tutto il ciclo di vita dei sistemi di Intelligenza Artificiale dello stato di diritto, dei diritti umani e dei valori democratici, che includono libertà, dignità ed autonomia, protezione dei dati, non discriminazione, uguaglianza, diversità, equità, giustizia sociale e lavoro.

[113] Così, S. QUATTROCOLO, *Intelligenza artificiale e giustizia*, op. cit., p. 4.

[114] Cfr. X. RONSIN – V. LAMPOS (a cura di), *Appendice I*, cit., Punto 34.a, p. 19.

[115] Cfr. *Idem*, Punto 34.d, p. 20. Condivide le preoccupazioni espresse dalla CEPEJ, cfr. S. QUATTROCOLO, *Intelligenza artificiale e giustizia*, op. cit., p. 5.

[116] CEPEJ, *Carta etica europea*, cit., p. 6.

[117] Cfr. *Idem*, Punto 133, p. 37.

dati siano concepiti e trattati in modo multidisciplinare[118] ed in un ambiente tecnologico sicuro, cioè ove non siano possibili loro modificazioni accidentali o strumentali fino a quando non siano stati effettivamente utilizzati nel meccanismo di apprendimento automatico (intangibilità del dato). Allo stesso modo, l'intero processo dovrebbe essere tracciabile per garantire che non vi siano state modifiche che possano aver alterato il contenuto o il significato della decisione in corso di elaborazione.

Il rispetto del terzo principio crea frizioni con il profilo della protezione del segreto industriale e commerciale del *software* e comporta la necessità di trovare un bilanciamento tra la tutela degli interessi commerciali ed il diritto di accedere ai codici che regolano un dispositivo di intelligenza artificiale[119].

Il quarto principio è quello di trasparenza, imparzialità ed equità (art. 4). Anche se all'apparenza presenta notevoli analogie con il secondo principio di non discriminazione, mentre i suoi elementi di imparzialità ed equità indicano come il dispositivo di IA dovrebbe funzionare (lettura in positivo), il principio di non discriminazione pone un divieto circa gli esiti della sua elaborazione (lettura in negativo). La trasparenza, invece, comporta sia che si possa conoscere come il dispositivo di IA è costruito (trasparenza tecnica) sia la possibilità di sapere chiaramente come si è giunti ad una certa elaborazione dei dati (trasparenza decisionale). La Carta etica afferma la necessità di raggiungere «un equilibrio tra la proprietà intellettuale di alcune metodologie di trattamento e l'esigenza di trasparenza (accesso al processo creativo), imparzialità (assenza di pregiudizi), equità e integrità intellettuale (privilegiare gli interessi della giustizia) quando si utilizzano strumenti che possono avere conseguenze giuridiche, o che possono incidere significativamente sulla vita delle persone»[120]. I tre principi, coniugati in un unico concetto, comportano che i metodi di trattamento dei dati siano accessibili e comprensibili[121] e la possibilità per Autorità o esperti indipendenti di certificare e verificare i metodi di trattamento e fornire

---

[118] Come è stato osservato, C. CASTELLI – D. PIANA, *Giusto processo e intelligenza artificiale*, Maggioli Editore, Rimini 2019, p. 89, «i dati resi disponibili per via della digitalizzazione non sono di per sé alcuna cosa se non sono prima strutturati in architetture organizzate ed intelligenti, e, in seconda battuta, analizzati avendo in mente domande, correlazioni, punti focali»; ciò perché «gli algoritmi non analizzano atti, analizzano la trascrizione in codici dei contenuti digitali di questi atti». Di qui la necessità di garantire la collaborazione tra operatori giudiziari e delle scienze sociali e gli sviluppatori di sistemi; cfr. A. ZIROLDI, *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in www.questionegiustizia.it, 18 ottobre 2019, p. 4 (reperibile *online* al collegamento https://www.questionegiustizia.it/articolo/intelligenza-artificiale-e-processo-penale-tra-norme-prassi-e-prospettive-_18-10-2019.php, consultato da ultimo in data 21 giugno 2022).

[119] Cfr., *ex multis*, R. ANGELINI, *Intelligenza Artificiale e* governance. *Alcune riflessioni di sistema*, in F. PIZZETTI (a cura di), *Intelligenza artificiale*, op. cit. p. 312.

[120] CEPEJ, *Carta etica europea*, cit., p. 11.

[121] Sulla stessa falsariga, l'OCSE, *Principles on Artificial Intelligence*, cit., Punto 1.3, p. 8, richiede agli addetti ai lavori trasparenza ed esplicabilità («*explanability*», da intendersi anche come leggibilità) col fine consentire agli interessati di intendere il risultato dell'attività di elaborazione dei sistemi di IA e di contestarne i risultati sulla base di informazioni di facile comprensione.
Sul tema del diritto alla spiegazione nella decisione automatizzata, si veda U. PAGALLO, *Algoritmi e conoscibilità*, in *Rivista di filosofia del diritto*, n. 1/2020, pp. 93-106.

preventivamente pareri[122]. Quando vengono utilizzati strumenti che possono avere conseguenze legali o che possono incidere significativamente sulla vita delle persone, è necessario che tali principi siano sempre presenti nell'intera catena progettuale ed operativa. Tuttavia, come è stato osservato, «non si può negare che l'istanza di segretezza dei codici-sorgente sia del tutto priva di rilievo, non solo con riguardo agli interessi commerciali, ma anche per esigenze interne al procedimento penale, quando si tratti di strumenti utilizzati a fini investigativi»[123].

Per quanto riguarda il rapporto tra trasparenza e privativa industriale, la stessa Carta etica richiama in nota[124] le osservazioni del Comitato di esperti sugli Intermediari Internet del Consiglio d'Europa, secondo cui «*The provision of entire algorithms or the underlying software code to the public is an unlikely solution in this context, as private companies regard their algorithm as key proprietary software that is protected. However, there may be a possibility of demanding that key subsets of information about the algorithms be provided to the public, for example which variables are in use, which goals the algorithms are being optimised for, the training data and average values and standard deviations of the results produced, or the amount and type of data being processed by the algorithm*»[125].

L'ultimo enunciato (art. 5) è specificamente finalizzato a «precludere un approccio [deterministico] e assicurare che gli utilizzatori siano soggetti informati ed abbiano il controllo delle loro scelte»[126], di modo da avvisare gli utenti su opportunità e rischi legati all'utilizzo dell'IA e porre al centro del sistema la volontà umana. Infatti, l'obiettivo dei dispositivi di intelligenza artificiale non deve essere quella di limitare l'autonomia decisionale dell'utente, ma di accrescerla.

Il principio del controllo da parte dell'utilizzatore («*under user control*») ha delle ricadute

---

[122] Nel settore della giustizia, specie penale, la creazione di Autorità indipendenti che possano verificare e certificare a priori l'efficienza ed efficacia dei modelli algoritmici utilizzati dai dispositivi è fondamentale per salvaguardare il principio fondamentale della pubblicità del processo decisionale a cui il giudice è tenuto in sede di motivazione della sentenza. Cfr. S. QUATTROCOLO, *Intelligenza artificiale e giustizia*, op. cit., p. 8.

[123] S. QUATTROCOLO, *Intelligenza artificiale e giustizia*, op. cit., p. 8. Sul tema specifico del procedimento penale, della stessa autrice, *Equità del processo penale e* automated evidence *alla luce della Convenzione Europea dei Diritti dell'Uomo*, in *Revista italo-española de Derecho Procesal*, vol. 1, 2019, p. 118 (reperibile *online* al collegamento http://www.revistasmarcialpons.es/rivitsproc/article/view/591/594, consultato da ultimo in data 21 giugno 2022).

[124] CEPEJ, *Carta etica europea*, cit., p. 11.

[125] Tradotto: «In questo contesto la divulgazione al pubblico di interi algoritmi o del codice *software* basilare è una soluzione utopistica, in quanto le imprese private considerano i loro algoritmi un fondamentale *software* proprietario, che è protetto. Tuttavia, può esservi la possibilità di domandare che siano divulgate al pubblico informazioni parziali fondamentali in materia di algoritmi, per esempio quali siano le variabili utilizzate, quali siano gli obiettivi cui è finalizzata l'ottimizzazione degli algoritmi, i dati di apprendimento, i valori medi e gli scarti tipo dei risultati ottenuti, o la quantità e il tipo di dati trattati dall'algoritmo». Studio del Consiglio d'Europa, DGI (2017)12. – Committee of experts on Internet Intermediaries (MSI-NET), *Algorithms and Human Rights*, op. cit., p. 38. Analogamente, al paragrafo 99 della relazione cit. *AI in the UK: ready, willing and able?* si afferma che, assodato che ottenere la piena trasparenza tecnica per certi sistemi di IA è difficile, se non impossibile, in alcuni contesti questa deve essere obbligatoria.

[126] CEPEJ, *Carta etica europea*, Principio n. 5, p. 6. Testo in lingua originale: «*preclude a prescriptive approach and ensure that users are informed actors and in control of the choices made*».

differenti in relazione alla diversa categoria di utente alla quale si rivolge[127]. «L'esistenza e la diffusione, tra gli operatori della giustizia, di adeguata letteratura esplicativa e di un dibattito scientifico[128] che coinvolga anche i giuristi»[129] sono il presupposto per assicurare la tutela e l'autonomia dell'utente, a cui però devono seguire altre garanzie, modulate in relazione alla specifica attività che il servizio automatizzato fornisce. Infatti, i professionisti della giustizia dovrebbero sempre poter risalire alle informazioni elaborate dalla macchina e restare liberi di dissentire dal risultato da essa fornito, preferendo altra soluzione ritenuta più calzante alla particolarità del caso concreto. I destinatari della decisione automatizzata, invece, dovrebbero essere avvisati «con un linguaggio chiaro e comprensibile del carattere vincolante o meno delle soluzioni proposte dagli strumenti di intelligenza artificiale, delle diverse possibilità disponibili e del [loro] diritto di ricevere assistenza legale e di accedere a un tribunale»[130], nonché di poter contestare l'utilizzo di un ausilio automatizzato alla decisione giudiziale[131] e far giudicare il loro caso da un tribunale ai sensi dell'art. 6, CEDU (accesso alla giustizia, diritto ad un equo processo, diritto ad una difesa tecnica, ecc.).

Tutti questi presìdi sono alla base dei sistemi di giustizia nazionali e potrebbero essere incrinati da una diffusione superficiale e disattenta degli strumenti computazionali esistenti. Nell'appendice di accompagnamento alla Carta etica due studi hanno individuato gli specifici aspetti problematici[132] delle diverse applicazioni di sistemi di IA, quali: l'effettiva capacità di questi di riprodurre il pensiero giuridico e spiegare retrospettivamente il comportamento del giudice[133]; il rischio, in ambito penale, di regressione a dottrine deterministiche, che erano state superate da un approccio favorevole alla valutazione della condotta personale nello specifico caso concreto e, dunque, alla individualizzazione della relativa sanzione; l'accentuazione delle discriminazioni già esistenti; il rigido ed acritico imporsi della vincolatività del precedente e della stessa decisione automatizzata. Partendo da queste considerazioni, nella seconda Appendice la Carta etica suddivide i possibili utilizzi dell'intelligenza artificiale nei sistemi giudiziari in quattro categorie, in base al loro livello di compatibilità con i cinque principi: quelli da incoraggiare; quelli da considerare, ma

[127] Cfr. S. QUATTROCOLO, *Intelligenza artificiale e giustizia*, op. cit., p. 9; A. ZIROLDI, *Intelligenza artificiale e processo penale*, op. cit., p. 5.

[128] La Carta parla della necessità di prevedere «programmi di alfabetizzazione informatica». CEPEJ, *Carta etica europea*, cit., p. 12.

[129] Così, S. QUATTROCOLO, *Intelligenza artificiale e giustizia*, op. cit., p. 9.

[130] CEPEJ, *Carta etica europea*, cit., p. 12.

[131] Sul punto è intervenuto anche il già ricordato art. 22, co. 1 GDPR, che garantisce all'interessato il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato.

[132] Per una loro breve disamina, si veda S. QUATTROCOLO, *Intelligenza artificiale e giustizia*, op. cit., pp. 10-12.

[133] Afferma *Eadem*, p. 3, che «un sistema di intelligenza artificiale *non è* in grado di spiegare il ragionamento giuridico, ma può soltanto […] esprimere la verosimiglianza che il giudice propenda per una decisione analoga a quella già adottata in circostanze simili (senza escludere il rischio di correlazioni errate)». Sul punto, X. RONSIN – V. LAMPOS (a cura di), *Appendice I*, cit., pp. 27-30.

con l'adozione di considerevoli precauzioni metodologiche; quelli in relazione ai quali sarebbero necessari ulteriori studi scientifici; infine, quelli «da esaminare con le più estreme riserve»[134].

Gli strumenti che potrebbero già essere utilizzati senza apparenti rischi, portando un beneficio al sistema giudiziario, sono: banche dati volte al reperimento di fonti giuridiche basate su tecniche di apprendimento automatico per il trattamento del linguaggio naturale, che rappresentano «soluzioni di ricerca complementari alle attuali parole chiave o alla ricerca a testo intero»[135]; terminali (*chatbot*) per facilitare l'accesso al diritto; strumenti impiegati a fini amministrativi per monitorare le prestazioni dei tribunali e allocare efficientemente le risorse umane ed economiche disponibili.

Un utilizzo possibile, a fronte di significative precauzioni metodologiche, è accordato agli applicativi volti alla produzione di statistiche ed all'individuazione, dopo un esame preliminare dei criteri inseriti dall'interessato, di misure di risoluzione alternativa delle controversie in materia civile. Allo stesso modo, potrebbero diffondersi sistemi di risoluzione alternativa nelle controversie *online* (*Online Dispute Resolution* – ODR), a patto però che gli utilizzatori siano informati dell'automatizzazione del procedimento e possano dissentire eventualmente dal parere ed adire un vero tribunale ai sensi dell'art. 6, CEDU, nonché siano «previste forme di controllo, da parte dei tribunali dello Stato, della procedura di risoluzione delle controversie *online* e del suo esito»[136]. Inoltre, la Carta etica non scoraggia l'impiego di sistemi di polizia predittiva di individuazione dei luoghi in cui potrebbero essere commessi dei reati (*hotspot*), ma non manca di sottolinearne i potenziali effetti distorsivi.

Gli impieghi che richiedono ulteriori studi scientifici attengono invece alla profilazione dei giudici e alla previsione delle decisioni giudiziali. Allo stato, infatti, i sistemi di apprendimento automatico funzionano tramite la semplice individuazione di correlazioni statistiche tra gruppi di parole e sono dunque incapaci di spiegare i fattori causativi di una decisione o di effettuare vere e proprie analisi giuridiche.

Infine, la CEPEJ tratta degli strumenti di valutazione del rischio (*risk assessment tools*) utilizzati in ambito processuale penale e dei dispositivi di analisi della giurisprudenza volti a fornire un ausilio alla decisione giudiziale e, basandosi su sperimentazioni già effettuate e sui relativi studi, giunge alla conclusione di scoraggiarne l'introduzione in territorio europeo.

Nel complesso, la CEPEJ ha un atteggiamento pragmatico e non preclude l'impiego delle nuove tecnologie nei sistemi giudiziari: infatti, cerca di incoraggiarne uno sviluppo controllato, se del caso raccomandando estrema cautela o arrivando a sconsigliare l'introduzione di alcuni specifici

[134] CEPEJ, *Carta etica europea*, *Appendice II*, cit., p. 44.
[135] *Idem*, p. 42.
[136] *Idem*, p. 43.

strumenti di IA.

Sono proprio la pragmaticità e – punto su cui torna spesso la stessa CEPEJ – l'instaurazione tra ingegneri, programmatori e professionisti del diritto di un dialogo scevro sia di un eccessivo entusiasmo sia di un'aprioristica avversione nei confronti delle nuove tecnologie le vie per governare il diffondersi degli applicativi di IA e portare beneficio all'umanità.

Allo stato, quindi, «ogni forma di i.a. "nasce" per una finalità e viene predisposta in sintonia con il raggiungimento di specifici risultati derivanti da due elementi: la tipologia di dati scelti e lo scopo cui si vuole rispondere, attraverso una elaborazione e valutazione di queste informazioni e correlazioni che [– quale terzo elemento cruciale per l'uso dell'i.a. nel diritto e nel campo delle scelte socialmente rilevanti –] per essere accettabile deve essere "trasparente" senza atteggiarsi a buco nero in cui entrano dati ed escono valutazioni senza che siano esplicitati modalità e parametri di correlazione (la cd. *black box*)»[137].

1.4 IA e diritto alla prova: tentativi, ostacoli e quadro normativo di riferimento.

Come visto, i sistemi di IA sono ormai entrati nella nostra vita di tutti i giorni e sono utilizzati nei più disparati settori. Sebbene molteplici rischi di violazione dei diritti fondamentali siano stati rilevati ed aspramente criticati, soprattutto a causa dell'errata selezione dei dati impiegati per allenare i dispositivi di IA e di possibili errori nella scrittura degli algoritmi che li governano, il loro utilizzo trova sempre più diffusione nella prassi e ciò comporta la necessità di tutelare comunque i diritti toccati da decisioni derivanti dal loro impiego.

In Italia, questioni come quella concernente l'accesso alle modalità di funzionamento dell'algoritmo che sviluppa le decisioni automatizzate sono già state affrontate dal giudice amministrativo[138], che è stato chiamato a pronunciarsi sulla legittimità di una procedura di assunzioni dei docenti delle scuole secondarie organizzata dal Ministero dell'Istruzione e gestita da un sistema informatico per mezzo di un algoritmo[139]. Nel caso di specie, sono stati contestati

[137] In questi termini, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 54.

[138] Anche i giudici civili cominciano ad affrontare i problemi sollevati dal diffondersi dell'IA. Per esempio, la Cass. civ., sez. I, 19 marzo 2019, sentenza n. 7708, ha ritenuto legittima la pronuncia di una inibitoria volta a bloccare «con le adeguate misure tecniche di intelligenza artificiale l'accesso ad un video di contenuto illecito da qualsiasi indirizzo web (cd. *dynamic injunction*)».

[139] In generale, L. VIOLA, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in www.federalismi.it, n. 21/2018 (reperibile *online* al collegamento https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=37334&dpath=document&dfile=06112018220520.pdf&content=L%27intelligenza%2Bartificiale%2Bnel%2Bprocedimento%2Be%2Bnel%2Bprocesso%2Bamministrativo%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B, consultato da ultimo in data 21 giugno 2022); specificamente, *ex multis*, F. PATRONI GRIFFI, *La decisione robotica e il giudice amministrativo*, in A. CARLEO (a cura di), *Decisione robotica*, il Mulino, Bologna 2019, pp. 165-178.

l'irrazionalità dell'assegnazione delle sedi di servizio per i candidati utilmente posti in graduatoria, perché effettuata senza tenere conto delle preferenze indicate dai soggetti interessati, il difetto di motivazione dei provvedimenti finali e la mancanza di trasparenza della procedura. Il Consiglio di Stato, Sez. VI, con sentenza n. 2270/2019[140], nel mettere in luce gli effetti favorevoli della digitalizzazione dell'attività amministrativa, il cui utilizzo deve essere incoraggiato, ha tracciato al contempo lo statuto dell'algoritmo nel procedimento. Infatti, se, da un lato, l'automazione del processo decisionale è sicuramente un metodo attraverso il quale la PA può raggiungere l'obiettivo costituzionale del buon andamento dell'azione amministrativa (art. 97 Cost.), dall'altro, ciò non può andare a scapito dei tradizionali principi che regolano l'attività amministrativa[141], quali la pubblicità, la trasparenza, la ragionevolezza, la proporzionalità ed il contemperamento di interessi contrapposti, né esula la stessa amministrazione a controllare e perfezionare l'algoritmo. Ne consegue che l'algoritmo deve poter essere analizzato e valutato dalle parti interessate all'esito del procedimento amministrativo[142] e, se del caso, sindacato dal giudice amministrativo, «al fine di poter valutare la correttezza del processo informatico e la logicità e la ragionevolezza [delle istruzioni] che governa[no] l'algoritmo»[143].

Per di più, l'intelligenza artificiale, oltre che nel campo prettamente scientifico e amministrativo, oggi rileva anche come strumento di ausilio per gli operatori giuridici. Nell'ambito del diritto civile sono già realtà l'uso di dispositivi di IA che facilitano l'accesso al patrimonio giurisprudenziale, redigono e controllano contratti e documenti e, cercando delle costanti decisionali tra un'enorme mole di sentenze, supportano le attività di consulenza di studi legali e compagnie assicurative, prevedendo quali potrebbero essere gli esiti di un'azione giudiziaria[144].

---

[140] In tema, I.A. NICOTRA – V. VARONE, *L'algoritmo, intelligente ma non troppo*, in *Rivista AIC*, n. 4/2019, pp. 86 e ss. (reperibile *online* al collegamento https://www.rivistaaic.it/images/rivista/pdf/4_2019_Nicotra_e_Varone.pdf, consultato da ultimo in data 21 giugno 2022). Per la sentenza di prime cure, TAR Lazio, Sez. III-bis, sent. 22 marzo 2017, n. 3769.

[141] Il principio secondo cui «l'utilizzo di procedure informatizzate non può essere motivo di elusione dei princìpi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa» è stato successivamente ribadito dal Consiglio di Stato in alcune decisioni che confermano, anche attraverso il rinvio a richiami testuali, quanto già sancito nella sentenza n. 2270 dell'8 aprile 2019 (cfr. Consiglio di Stato, Sez. VI, sentt. 13 dicembre 2019, nn. 8472, 8473 e 8474). Per un breve commento alla sentenza n. 8472, si veda M. IASELLI, *Algoritmi in ambito amministrativo, il Consiglio di Stato delinea i limiti*, in www.altalex.com, 20 gennaio 2020 (reperibile *online* al collegamento https://www.altalex.com/documents/news/2020/01/20/algoritmi-in-ambito-amministrativo-il-consiglio-di-stato-delinea-i-limiti, consultato da ultimo in data 21 giugno 2022). Invece, per un'analisi generale dell'orientamento del Consiglio di Stato sulle decisioni algoritmiche, si veda J. DELLA TORRE, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Rivista di diritto processuale*, n. 2/2021, pp. 713 e ss.

[142] Ne consegue anche l'utilizzo da parte della PA di *software* basati su banche dati libere a scapito di quelli a cui si applica la disciplina sui diritti di proprietà intellettuale, che è di ostacolo, *in primis*, ai principi di pubblicità e trasparenza.

[143] Così, F. DONATI, *Intelligenza artificiale e giustizia*, in C. BERTOLINO – T. CERRUTI – M. OROFINO – A. POGGI, *Scritti in onore di Franco Pizzetti*, Vol. II, Edizioni Scientifiche Italiane, 2020, p. 389.

[144] Tra i più diffusi programmi predittivi di assistenza legale, si segnalano, per esempio, il Watson/ROSS intelligence dell'IBM (per la presentazione del sistema ROSS, si veda il sito https://blog.rossintelligence.com/, consultato da ultimo in data 21 giugno 2022) ed il francese Prédictive, che permettono ad avvocati e consulenti di conoscere le probabilità di successo di una causa.

Come passo successivo, partendo dal postulato secondo il quale decisioni rese su situazioni a priori comparabili non possono che essere uniformi, si è pensato di adottare sistemi di giustizia predittiva nel campo giudiziario[145] per supportare i giudici nel momento decisorio e, addirittura, per sostituirne totalmente l'operato, con l'intento di «rendere più efficiente, più equo e meno costoso il funzionamento del sistema giustizia»[146]. Al raggiungimento di tale obiettivo ha spinto anche il riaffiorare della corrente di pensiero del formalismo giuridico, che vorrebbe arginare il crescente ruolo che la magistratura è andata ritagliandosi in ambito interpretativo (*in primis*, per il formalismo giuridico bisogna diffidare della discrezionalità della decisione umana); soprattutto, oggetto di critica di questa corrente è l'imporsi dei giudici quale autonoma fonte creatrice di diritto, in quanto tale situazione andrebbe a danno della certezza del diritto[147] e della tradizionale divisione dei poteri. Proprio in quest'ottica si inserisce il tentativo di concretizzare l'idea montesquieuiana del giudice-automa, che, quale «*être inanimé*»[148], non farebbe altro che applicare le disposizioni normative redatte dall'assemblea rappresentativa eletta dal popolo attraverso una semplice operazione logica di sussunzione della fattispecie concreta a quella astratta prevista dalla legge: la «logica giuridica [coinciderebbe quindi] con la logica formale e il giudice, senza dispiegare discrezionalità alcuna e alcun potere, e prendendo le distanze dalle proprie opinioni, dalle proprie convinzioni etiche e dalle proprie emozioni, si [comporterebbe] proprio in modo simile ad una macchina»[149].

Se tutti sono, comunque, concordi sull'impossibilità di creare un «giudice-macchina», in quanto l'attività giurisprudenziale è inevitabilmente creativa, l'ambizione è ora quella di creare una «macchina-giudice», capace di interpretare meccanicamente la legge ed essere così mera *bouche de la loi*[150]. Nei fatti, però, alla realizzazione di tale progetto si frappongono limiti tecnici e giuridici.

---

[145] Sul rapporto tra intelligenza artificiale, giustizia predittiva, processo e sentenza "robotica", si vedano, *ex multis*, i contributi raccolti in A. CARLEO (a cura di), *Decisione robotica*, op. cit.; J. NIEVA-FENOLL, *Intelligenza artificiale e processo*, Giappichelli, Torino 2019, ed ivi ampia bibliografia sul tema; D. DALFINO, *Stupidità (non solo) artificiale, predittività e processo*, in www.questionegiustizia.it, 3 luglio 2019 (reperibile *online* al collegamento https://www.questionegiustizia.it/articolo/stupidita-non-solo-artificiale-predittivita-e-processo_03-07-2019.php, consultato da ultimo in data 21 giugno 2022); L. D'AGOSTINO, *Sicurezza informatica, compliance e prevenzione del rischio di reato*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2019, pp. 354-373 (reperibile *online* al collegamento https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_dagostino.pdf, consultato da ultimo in data 21 giugno 2022).

[146] Così, F. DONATI, *Intelligenza artificiale e giustizia*, op. cit., p. 379.

[147] Già Max Weber sosteneva che tra le condizioni necessarie per lo sviluppo del modello capitalista ci fosse l'esistenza di un diritto calcolabile. Cfr. F. DONATI, *ult. cit.*, p. 379 e F. CERESA GASTALDO, *Il giudice-robot*, op. cit., p. 2.

[148] Tradotto: «Essere inanimato», da intendersi anche come «spersonalizzato». C. MONTESQUIEU, *Esprit des Lois*, Libro XI, cap. VI, 1798. Il passo completo – nel quale viene definito il compito del giudice – da cui si trae la citazione è il seguente: «*Les juges de la nation ne sont que la bouche qui prononce les paroles de la loi, des êtres inanimés, qui n'en peuvent modérer ni la force ni la rigueur*» (tradotto: «I giudici della Nazione non sono che la bocca che pronuncia le parole della legge, degli esseri inanimati, che non possono moderare né la forza, né il rigore»).

[149] Così, F. CERESA GASTALDO, *Il giudice-robot*, op. cit., p. 3.

[150] Cfr. *Eadem*, p. 5. Ad esempio, in un progetto pilota in Estonia le cause civili per un valore inferiore di 7.000 euro saranno decise da specifici programmi, salva la possibilità di appello; cfr. C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 51.

Dal punto di vista tecnico, gli odierni sistemi di apprendimento automatico si limitano a individuare le connessioni che legano degli elementi contenuti nella sentenza e nel dispositivo e proporre le stesse soluzioni ai nuovi casi che presentano le stesse caratteristiche; questo perché non sono in grado di replicare il ragionamento giudiziale con l'applicazione deduttiva di regole predeterminate e l'attribuzione di significato alle norme attraverso l'utilizzo anche di elementi extra-giuridici[151]. Altro limite da considerare riguarda invece l'eventualità che i dispositivi di IA, nello svolgere determinate funzioni, riproducano gli errori e i pregiudizi insiti nel pensiero umano: infatti, ciò pone un ostacolo all'ambizione di avvalersi di strumenti tecnici, quindi presumibilmente neutri e oggettivi, per eliminare ogni tipo di influenza nell'*iter* decisorio[152]. Infine, nei sistemi di diritto continentale, c'è il rischio che si imponga un sistema fondato sul precedente, per di più, diversamente da quanto accade nei sistemi di *common law*, caratterizzato da «rigidità e incapacità di evoluzione»[153].

Anche dal punto di vista giuridico sorgono problemi. Calandoci nello specifico sistema istituzionale italiano, l'idea che un dispositivo di IA possa sostituirsi al giudice-persona non può essere ammessa per la contrarietà ai nostri principi costituzionali. In tal senso, l'art. 25 Cost., nel garantire il diritto al «giudice naturale precostituito per legge», fa evidentemente riferimento ad un giudice-persona. L'«ingresso degli algoritmi nella struttura della decisione giudiziale […] profila inoltre un problema di rispetto del principio democratico e di trasparenza con ricadute sensibili anche sulla tenuta del principio di riserva di legge (art. 25/2 Cost.), visto che l'algoritmo si affianca ed integra la legge, secondo il principio "*code is law*"»[154]: infatti, nel diritto penale si assiste al fenomeno per cui «il primato delle norme incriminatrici disposte dalla legge viene sostituito dalle norme che regolano l'applicazione del *software*»[155].

Sempre sul piano sostanziale, l'uso di algoritmi determinerebbe lo slittamento dalla materialità e offensività del reato e dalla personalità della responsabilità penale alla figura dell'autore del reato. Dunque, è necessario «evitare il rischio che attraverso questi strumenti si apra

---

[151] Cfr. C. BARBARO, *Uso dell'intelligenza artificiale nei sistemi giudiziari*, op. cit., pp. 191-192. Secondo uno studio condotto dall'University College of London (UCL) su una macchina di apprendimento automatico, la macchina, apprendendo da una serie di decisioni della Corte EDU, «non ha cercato di simulare un ragionamento giuridico; ha, semplicemente, provveduto al trattamento statistico dei dati raccolti e calcolato delle probabilità». L'esperimento è menzionato, *ex multis*, in X. RONSIN – V. LAMPOS (a cura di), *Appendice I*, cit., p. 28 e F. CERESA GASTALDO, *Il giudice-robot*, op. cit., p. 10.

[152] Cfr., *ex multis*, F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Harvard University Press, Cambridge - London 2015.

[153] In questi termini, F. CERESA GASTALDO, *Il giudice-robot*, op. cit., p. 7.

[154] Così, V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in www.discrimen.it, 15 maggio 2020, p. 13 (reperibile *online* al collegamento https://discrimen.it/wp-content/uploads/Manes-Loracolo-algoritmico-e-la-giustizia-penale.pdf, consultato da ultimo in data 21 giugno 2022); il contributo è stato pubblicato anche nel volume U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, op. cit., pp. 547-569.

[155] In questi termini, F. SGUBBI, *Il diritto penale totale. Punire senza legge, senza verità, senza colpa. Venti tesi*, il Mulino, Bologna 2019, p. 41.

la strada a una forma inaccettabile di determinismo penale, per cui dal diritto penale del fatto – sancito dall'art. 25, comma 2, Cost. – si passi a un inaccettabile diritto penale del profilo d'autore, nel quale la pericolosità di un soggetto viene desunta esclusivamente dagli schemi comportamentali e dalle decisioni assunte in una determinata comunità del passato», che del resto «sarebbe contrario al principio di individualizzazione del trattamento sanzionatorio, desumibile dall'art. 27, commi 1 e 3, Cost., nonché, del canone di individualizzazione del trattamento cautelare, ricavabile dagli artt. 13 e 27, comma 2, Cost.»[156]. D'altronde, lo stesso art. 220, co. 2 c.p.p., vietando nel giudizio di cognizione il ricorso alla perizia «per stabilire l'abitualità o la professionalità nel reato, la tendenza a delinquere, il carattere e la personalità dell'imputato» col fine di evitare che «il giudicante possa rimanere condizionato dalle valutazioni sul carattere dell'imputato, tralasciando di apprezzare adeguatamente il fatto oggetto di giudizio»[157], si pone come baluardo all'ingresso di certi tipi di strumenti di valutazione del rischio[158] nel sistema processuale italiano.

L'art. 101, co. 1 Cost., nell'affermare che i «giudici sono soggetti soltanto alla legge», esclude la possibilità che il giudice, applicandola passivamente, si adagi sul risultato di un'elaborazione algoritmica e, *lato sensu*, vieta che la funzione giudicante sia lasciata totalmente ad un dispositivo elettronico. Allo stesso risultato si arriva considerando l'art. 102: infatti, se la «funzione giurisdizionale è esercitata da magistrati ordinari istituiti e regolati dalle norme sull'ordinamento giudiziario», ne consegue il divieto di demandarla ad un algoritmo, che non rientra nella categoria individuata.

Allo stato della tecnica, un algoritmo non potrebbe ricoprire il ruolo di «giudice terzo e imparziale» come richiesto dall' art. 111, 2 co. Cost., a causa del forte rischio che le sue decisioni siano viziate da pregiudizi innescati dalla considerazione di alcuni fattori e non altri; violazione, tra l'altro, che porrebbe anche un problema nella prospettiva del rispetto del diritto di uguaglianza (art. 3, Cost). La garanzia del diritto di ogni cittadino al un giudice indipendente e imparziale è del resto ribadita anche dalla CEDU (art. 6, comma 1) e dalla Carta dei diritti fondamentali dell'Unione europea.

Proseguendo, si avvertono rischi di violazione degli artt. 24, co. 2 e 111, co. 6 Cost., che riguardano rispettivamente il diritto di difesa e l'obbligo di motivazione dei provvedimenti

---

[156] Così, M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, op. cit., p. 21.

[157] In questi termini, L. MALDONATO, *Algoritmi predittivi e discrezionalità del giudice: una nuova sfida per la giustizia penale*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2019, p. 411 (reperibile *online* al collegamento https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_maldonato.pdf, consultato da ultimo in data 21 giugno 2022).

[158] Come si vedrà più avanti, nello specifico caso del dispositivo COMPAS, all'imputato vengano richieste informazioni sulla propria personalità e il proprio carattere per permettere l'elaborare di un risultato sul rischio di recidivanza dello stesso (l'intero questionario che viene sottoposto all'imputato è reperibile *online* al collegamento https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html, consultato da ultimo in data 21 giugno 2022).

giurisdizionali. Nello specifico, non conoscendosi le modalità di funzionamento del *sofware*, le parti dovrebbero confrontarsi con una decisione priva di motivazione o con motivazione meramente apparente, e ciò avrebbe ricadute sul rispetto dei principi dell'equo processo e del diritto di difesa (e del loro corollario della parità delle armi)[159].

In definitiva, come è stato osservato, si può giungere alla conclusione per cui «l'impiego dell'IA al posto del giudice inciderebbe sulle garanzie costituzionali attinenti alla giurisdizione, quali l'effettività e la pienezza del diritto alla difesa delle parti, la qualità della decisione giurisdizionale, la capacità del giudice di far emergere la irriducibile peculiarità dei fatti e di calibrare su di essi la decisione, l'obbligo di motivazione»[160].

Dunque, per i motivi brevemente accennati[161] e sperimentazioni conclusesi con risultati negativi[162], allo stato gran parte della dottrina[163] e degli operatori del diritto concordano nell'affermare che affidare ad un sistema di apprendimento automatico il compito di decidere non è sensato, ma non mancano ugualmente tentativi in tal senso. Ad esempio, in Cina, pure dove le questioni etiche sono valutate in modo diverso rispetto al mondo occidentale, si può notare un orientamento ondivago: da un lato, viene ribadito il ruolo dell'uomo nella funzione giudicante, anche a fronte dell'implementazione di apparati dematerializzati e digitali come la Beijing Internet Court, un sistema di supporto decisionale per il giudice di primo grado per le controversie riguardanti e nate in Internet[164]; dall'altro, invece, a Shangai alcune fattispecie di reato saranno gestite in totale autonomia dall'algoritmo System 206, che stabilirà l'innocenza o la colpevolezza degli imputati ed irrogherà le conseguenti pene[165].

---

[159] Cfr. S. QUATTROCOLO, *Equità del processo penale*, op. cit., pp. 119-120.

[160] Così, F. DONATI, *Intelligenza artificiale e giustizia*, op. cit., p. 395.

[161] Per approfondire, si vedano A. TRAVERSI, *Intelligenza artificiale applicata alla giustizia,* op. cit.; L. VIOLA (a cura di), *Giustizia predittiva e interpretazione della legge con modelli matematici. Atti del Convegno tenutosi presso l'Istituto dell'enciclopedia Italiana Treccani*, Diritto Avanzato, Milano 2019.

[162] Si fa riferimento, tra gli altri, anche agli esperimenti svolti in Francia presso le Corti di appello di Rennes e di Douai. Cfr. S. GABORIAU, *Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?*, in www.questionegiustizia.it, n. 4/2018, pp. 201-203 (reperibile *online* al collegamento https://www.questionegiustizia.it/rivista/2018-4.php, consultato da ultimo in data 21 giugno 2022); X. RONSIN – V. LAMPOS (a cura di), *Appendice I*, cit., pp. 30-31.

[163] Altri, invece, pur criticando la tesi della previsione su base statistica-giurisprudenziale, non abbandonando l'idea di adottare un sistema di giustizia predittiva, proponendo invece di optare per un modello deduttivo (previsione su base algoritmico-normativa tramite combinazione di dati); cfr. L. VIOLA, *Giustizia predittiva: è preferibile un modello deduttivo*, in www.altalex.com, 10 marzo 2020 (reperibile *online* al collegamento https://www.altalex.com/documents/news/2020/03/10/giustizia-predittiva-preferibile-modello-deduttivo, consultato da ultimo in data 21 giugno 2022).

[164] Per la Beijing Internet Court, si veda il sito https://english.bjinternetcourt.gov.cn/index.html, consultato da ultimo in data 21 giugno 2022.

[165] Notizia riportata dal *South China Morning Post* (cfr. S. CHEN, *Chinese scientists develop AI 'prosecutor' that can press its own charges*, 26 dicembre 2021, reperibile *online* al collegamento https://www.scmp.com/news/china/science/article/3160997/chinese-scientists-develop-ai-prosecutor-can-press-its-own?module=perpetual_scroll_0&pgtype=article&campaign=3160997, consultato da ultimo in data 21 giugno 2022) e ripresa dalla stampa italiana: cfr., *ex multis*, V. ERRANTE, *Cina, arrivano i robot-magistrati. Ora ti accusa un algoritmo: «Decide col 97% di precisione»*, in www.ilmessaggero.it, 2 gennaio 2022 (reperibile *online* al collegamento

Nonostante i limiti e divieti detti per la fase decisoria, sarebbe, comunque, un errore non sfruttare le opportunità date dall'IA per sostenere e migliorare l'efficacia del lavoro giudiziario e dare delle indicazioni sul possibile esito delle controversie giudiziarie[166]. In questa direzione, come già accennato, vanno *chatbot* per orientare il cittadino verso una soluzione di risoluzione alternativa della controversia (Lettonia) e dispositivi per facilitare il lavoro di cancelleria (adottati in Austria) o per la gestione *online* di casi di mediazione delle controversie riguardanti il diritto di famiglia ed altre materie (in Olanda)[167].

In Italia, invece, pur essendo stata completata la realizzazione del processo telematico nel campo del diritto civile e amministrativo[168], che permette il controllo automatizzato sulla ammissibilità del deposito di atti e documenti, ed avendo assistito a tentativi insoddisfacenti di rendere matematicamente calcolabili le conseguenze derivanti da un'azione giudiziaria[169], «non è dato rilevare un concreto e significativo utilizzo di sistemi di IA da parte dei giudici»[170]. Gli unici progetti in atto, tralasciati gli strumenti digitali di videoscrittura e banche dati già a disposizione delle aule di giustizia[171], riguardano i tentativi di alcuni Tribunali e Corti di Appello[172] – tra le altre,

---

https://www.ilmessaggero.it/mondo/cina_magistrati_robot_algoritmo_processo_virtuale_cosa_sappiamo-6415043.html, consultato da ultimo in data 21 giugno 2022); M. BORGOBELLO, *Il procuratore "robot" debutta in Cina: così l'IA ora elabora le accuse*, in www.agendadigitale.eu, 14 gennaio 2022 (reperibile *online* al collegamento https://www.agendadigitale.eu/documenti/giustizia-digitale/il-procuratore-virtuale-debutta-in-cina-cosi-lia-ora-elabora-le-accuse/, consultato da ultimo in data 21 giugno 2022); M. ROVELLI, *L'intelligenza artificiale in tribunale: dal giudice robot in Cina alle sperimentazioni in Italia*, in www.corriere.it, 3 marzo 2022 (reperibile *online* al collegamento https://www.corriere.it/tecnologia/22_marzo_03/intelligenza-artificiale-tribunale-giudice-robot-cina-sperimentazioni-italia-52150de6-9977-11ec-9c59-6d8197f09466.shtml, consultato da ultimo in data 21 giugno 2022).

[166] Sulla macchina quale ausilio per il giudice, si veda, *ex multis*, U. RUFFOLO, *Giustizia predittiva e* machina sapiens *quale "ausiliario" del giudice umano*, in www.astrid-online.it, fasc. n. 8/2021 (reperibile *online* al collegamento https://www.astrid-online.it/static/upload/protected/astr/astrid_ruffolo-u_03_05_21.pdf, consultato da ultimo in data 21 giugno 2022).

[167] La piattaforma Rechtwijzer (raggiungibile al collegamento https://rechtwijzer.nl/, consultato da ultimo in data 21 giugno 2022), frutto della collaborazione tra l'Università di Twente e di Hiil (Hague Institute for the Internationalisation of the Law), permette la connessione tra utente, mediatore e assistente legale, in via totalmente digitale e dematerializzata, e fornisce servizi di consulenza, mediazione e monitoraggio della fase esecutiva. Per un'analisi sui risultati – ritenuti non soddisfacenti – ottenuti dalla piattaforma, si veda M. BARENDRECHT, *Rechtwijzer: Why Online Supported Dispute Resolution Is Hard to Implement*, in www.hiil.org, 21 giugno 2017 (reperibile *online* al collegamento https://www.hiil.org/news/rechtwijzer-why-online-supported-dispute-resolution-is-hard-to-implement/, consultato da ultimo in data 21 giugno 2022).

[168] Per il processo amministrativo, cfr. Allegato A al D.P.C.M. 16 febbraio 2016, n. 40 (regolamento recante le regole tecnico-operative per l'attuazione del processo amministrativo telematico).

[169] Nel caso specifico, si trattava del tentativo del Tribunale di Firenze di utilizzare un sistema di calcolo, il MoCAM (Modello di Calcolo dell'Assegno di Mantenimento), per produrre una stima dell'assegno di mantenimento per i figli e, eventualmente, del contributo a favore del coniuge, nel caso di separazione, divorzio o rottura di una unione di fatto, e così ripartire in modo equo il danno economico derivante. Il sistema è stato abbandonato perché incapace di considerare la prassi e la giurisprudenza maturate nei Tribunali e apprezzare in termini di qualità e non solo di quantità dei compiti svolti dai genitori nei confronti dei figli. Cfr. F. DONATI, *Intelligenza artificiale e giustizia*, op. cit., pp. 381-382.

[170] Così, F. DONATI, *ult. cit.*, p. 381.

[171] Si pensi, per esempio, al Centro elettronico di documentazione (CED) della Corte di Cassazione.

[172] Cfr. C. CASTELLI, *Giustizia predittiva*, in www.questionegiustizia.it, 8 febbraio 2022 (reperibile *online* al collegamento https://www.questionegiustizia.it/articolo/giustizia-predittiva, consultato da ultimo in data 21 giugno 2022).

di Bari[173], Venezia[174] e Brescia[175] – di rendere accessibili schede tematiche sulla giurisprudenza consolidata su materie e casistiche ricorrenti, al fine di fornire agli utenti indicazioni circa il prevedibile esito di una possibile controversia in tali campi, nonché sul tempo necessario alla definizione della stessa. Oltre a non trattarsi sempre di dispositivi di IA rientranti nell'accezione qui utilizzata, questi sistemi di schede hanno anche il limite di non poter tener conto delle peculiarità di ogni singolo caso e di dover essere costantemente aggiornati con la giurisprudenza della Corte di Cassazione, della Consulta e delle Corti internazionali. Progetti di giustizia predittiva[176] per il giudice sembrano, però, già stati implementati della Scuola Superiore Sant'Anna di Pisa, in collaborazione con i tribunali di Genova e Pisa, o previsti dalla Corte di Cassazione[177] e dal Ministero della Giustizia[178] e da attuare con i fondi del PNRR (Piano Nazionale di Ripresa e Resilienza[179])[180].

---

[173] Circa la Terza Sezione civile della Corte d'Appello di Bari, il progetto «Prevedibilità delle decisioni» (reperibile *online* al collegamento http://www.corteappello.bari.it/allegati_sito/progetto_prevedibilita_decisioni.pdf, consultato da ultimo in data 21 giugno 2022) è stato approvato con decreto 5 ottobre 2016 del relativo presidente. Le schede sulla giurisprudenza e sulle tempistiche su specifiche materie sono reperibili *online* al collegamento https://www.corteappello.bari.it/buone_prassi_4.aspx, consultato da ultimo in data 21 giugno 2022.

[174] Per la Corte di Appello di Venezia, si veda il collegamento https://www.corteappello.venezia.it/giurisprudenza-predittiva-per_198.html, consultato da ultimo in data 21 giugno 2022.

[175] Sul tema, brevemente, C. MORELLI, *Giustizia predittiva: il progetto (concreto) della Corte d'appello di Brescia*, in www.altalex.com, 8 aprile 2019 (reperibile *online* al collegamento https://www.altalex.com/documents/news/2019/04/08/giustizia-predittiva#uno, consultato da ultimo in data 21 giugno 2022). Nel sito della Corte di Appello di Brescia si trovano gli albori di questo progetto (https://www.giustizia.brescia.it/giustizia_predittiva.aspx?pnl=2, consultato da ultimo in data 21 giugno 2022). Successivamente, Tribunale, Corte d'Appello e Università di Brescia hanno lanciato un sistema di giustizia predittiva (raggiungibile al collegamento https://giustiziapredittiva.unibs.it/, consultato da ultimo in data 21 giugno 2022), dove «scelta l'area tematica di interesse, si può percorrere, secondo un grado crescente di approfondimento, un "itinerario", guidato e teso ad individuare la vicenda giudiziaria più appropriata, per identità o similitudine, a quella di proprio interesse, "arrivando", alla fine di quell'itinerario, alla soluzione cercata».

[176] Sui benefici che il sistema giustizia potrebbe trarre da tali sistemi, si vedano C. CASTELLI – D. PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi*, in www.questionegiustizia.it, 15 maggio 2018, specialmente i parr. 2.1-2.4 (reperibile *online* al collegamento https://www.questionegiustizia.it/articolo/giustizia-predittiva-la-qualita-della-giustizia-in-due-tempi_15-05-2018.php, consultato da ultimo in data 21 giugno 2022); riguardante l'ambito penale, cfr. C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., pp. 63-66.

[177] Cfr. C. MORELLI, *L'Intelligenza artificiale entra in Corte di Cassazione*, in www.altalex.com, 18 ottobre 2021 (reperibile *online* al collegamento https://www.altalex.com/documents/news/2021/10/18/intelligenza-artificiale-entra-in-corte-di-cassazione, consultato da ultimo in data 21 giugno 2022).

[178] Il Ministero della Giustizia, per il tramite della Direzione generale per i sistemi informativi automatizzati (DGSIA), ha reso noto nel sito istituzionale (https://www.giustizia.it/giustizia/it/mg_2_20_3.page#, consultato da ultimo in data 21 giugno 2022) un progetto, da realizzarsi in collaborazione con la Conferenza dei Rettori (CRUI), per mettere a disposizione degli operatori degli strumenti di IA da utilizzare come ausilio alle loro mansioni. Cfr. DGSIA, *Ricognizione della digitalizzazione del processo civile e penale e della transizione digitale del ministero della giustizia*, febbraio 2021 (reperibile *online* al collegamento https://www.giustizia.it/cmsresources/cms/documents/studio_dgsia_ricognizione_digitalizzazione_febbraio2021.pdf, consultato da ultimo in data 21 giugno 2022).

[179] L'Unione europea ha risposto alla crisi legata alla pandemia di COVID-19 con il Next Generation EU (NGEU). Uno degli strumenti del NGEU è il Dispositivo per la Ripresa e Resilienza (RRF), che richiede agli Stati membri di presentare un pacchetto di investimenti e riforme: appunto, il Piano Nazionale di Ripresa e Resilienza (PNRR). Il Piano italiano è reperibile *online* al collegamento https://www.governo.it/sites/governo.it/files/PNRR.pdf, consultato da ultimo in data 21 giugno 2022. Circa le riforme previste nel campo della giustizia, si vedano le pp. 47 e ss.; invece, in merito all'utilizzo specifico di dispositivi di IA, vagamente p. 58, ove si dice che i «progetti presentati nell'ambito del PNRR […] consentono di declinare sotto diversi aspetti l'azione riorganizzativa della macchina giudiziaria e amministrativa con il fine principale di: […] Aumentare il grado di digitalizzazione della giustizia mediante l'utilizzo di strumenti

Sulla scorta di quanto già avviene presso la Cassazione e le Corti d'Appello e, in Europa, presso la Corte di giustizia, ove la figura dell'Avvocato generale, un magistrato togato e indipendente, fornisce al collegio giudicante la propria opinione non vincolante sul caso ad esso sottoposto, tra le proposte avanzate nell'ottica di ausilio e maggiore certezza del sistema[181] vi è, per esempio, la costruzione di «un sistema che salvaguardi il primato della decisione umana e la assoluta libertà di giudizio del giudice-uomo, e però gli affianchi, con funzione servente ma ritualizzata, una sorta di Avvocato Generale-macchina, le cui "conclusioni" costituiscano un "parere" obbligatorio ma non vincolante, un progetto di sentenza che il giudice umano resta libero di disattendere, ma con decisione motivata»[182]. I vantaggi di tale strumentazione starebbero nella possibilità del giudice-persona di confrontarsi con un progetto decisione elaborato velocemente, ricco di dati e rispettoso del precedente (in favore della prevedibilità), con l'assoluta possibilità di discostarsene, se le esigenze del caso concreto o il diverso sentire della società circa un determinato tema – non considerabili dalla macchina – lo richiedono.

Anche se vi è apertura per l'introduzione di dispositivi di IA con funzione ancillare per il giudice, la necessità di prendere le dovute precauzioni non viene meno. In ambito penale, studi sull'esperienza del ricorso a sistemi di valutazione automatizzata di predizione del rischio di recidiva (*risk assessment tools*) «hanno […] rilevato la possibilità che il loro impiego non adeguatamente controllato inneschi l'introduzione di pregiudizi di ordine razziale o comunque relativi all'appartenenza a determinati contesti»[183]: come dimostra la vicenda dello specifico dispositivo COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*)[184], possono essere riprodotti dei pregiudizi insiti nella società, mancando così l'obiettivo di giungere ad un risultato scevro da condizionamenti circa la decisione da prendere su una determinata

---

evoluti di conoscenza (utili sia per l'esercizio della giurisdizione sia per adottare scelte consapevoli), il recupero del patrimonio documentale, il potenziamento dei software e delle dotazioni tecnologiche, l'ulteriore potenziamento del processo (civile e penale) telematico». Dunque, si sottolinea come il Piano sorvoli sull'utilizzo dell'IA ed incentri maggiormente la riforma della giustizia nella semplice limitazione delle tempistiche delle varie fasi procedimentali. Per i dettagli dei progetti previsti, si veda la citata *Ricognizione della digitalizzazione del processo civile e penale* della DGSIA, pp. 53 e ss.

[180] Cfr. M. ROVELLI, *L'intelligenza artificiale in tribunale*, op. cit., parr. "*I progetti del Ministero della Giustizia*" e ss.

[181] Per ulteriori prospettive in tema di giustizia predittiva, si veda C. CASTELLI – D. PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi*, op. cit., par. 2.5.

[182] Così, U. RUFFOLO, Machina iuris-dicere potest*?*, in www.biodiritto.org, *BioLaw Journal – Rivista di BioDiritto*, n. 2/2021, p. 402 (reperibile *online* al collegamento https://teseo.unitn.it/biolaw/article/view/1673, consultato da ultimo in data 21 giugno 2022).

[183] In questi termini, A. ZIROLDI, *Intelligenza artificiale e processo penale*, op. cit., p. 4. Sul punto anche X. RONSIN – V. LAMPOS (a cura di), *Appendice I*, cit., Punti 133 e ss., pp. 37-38.

[184] Per la presentazione di COMPAS, elaborato e commercializzato dalla società Northpointe – Equivant, di veda il sito www.equivant.com, consultato da ultimo in data 21 giugno 2022. La guida sul funzionamento del dispositivo è reperibile *online* nel sito dell'azienda produttrice al collegamento https://www.equivant.com/wp-content/uploads/Practitioners-Guide-to-COMPAS-Core-040419.pdf, consultato da ultimo in data 21 giugno 2022). Sul funzionamento di COMPAS, brevemente, F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., pp. 19-20 e C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., pp. 69-70.

questione[185]. Nel caso assurto a paradigma del pericolo appena accennato *State v. Loomis*[186], la Corte Suprema del Wisconsin, chiamata ad esprimersi dal ricorrente sull'entità della pena inflittagli dalla Corte locale che, appunto avvalendosi del COMPAS, l'aveva ritenuto soggetto ad alto rischio di recidiva, «ha escluso che l'utilizzo del programma avesse violato il diritto dell'imputato a un equo processo»[187] e del principio di non discriminazione per due motivi. In primo luogo, la mancata trasparenza sui criteri utilizzati dal dispositivo per funzionare – la legge statunitense sulla tutela dei diritti di proprietà intellettuale non permette l'accesso ai codici sorgente su cui è impostato il *software* – non impedisce all'imputato di poter confutare la decisione elaborata da quest'ultimo sulla base di dati certi e conosciuti in entrata[188]. In secondo luogo, secondo la Corte, il giudice non può fondare la sua decisione esclusivamente sul risultato offerto da COMPAS: infatti, «*a COMPAS risk assessment is only one of many factors that may be considered and weighed at sentencing*»[189].

Nonostante la presa di posizione della Corte, nei confronti dell'algoritmo utilizzato dal COMPAS sono state sollevate alcune critiche in ordine alla sua effettiva validità predittiva (*accurancy*) e alla sua imparzialità (*fairness*)[190]. Nel 2016 l'organizzazione non governativa

---

[185] In ambito statunitense, altri strumenti di valutazione automatizzata di predizione del rischio di recidiva sono utilizzati in sede di decisione della cauzione (*bail*). Invece, in Inghilterra la polizia di Durham, in collaborazione con l'Università di Cambridge, ha messo a punto un sistema denominato HART (*Harm Assessment Risk Tool*) per valutare, verificando il rischio che il soggetto arrestato commetta dei reati nei due anni successivi, quando una persona può essere sottoposta a un programma di riabilitazione in alternativa all'esercizio dell'azione penale. In merito ad entrambi i punti, brevemente, M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, op. cit., pp. 8-12 e bibliografia ivi riportata. Specificamente su HART, si veda M. OSWALD – J. GRACE – S. URWIN – G. BARNES, *Algorithmic risk assessment policing models: lessons from the Durham HART model and "Experimental" proportionality*, in *Information & Communications Technology Law*, vol. 27, n. 2/2018, pp. 223-250 (reperibile *online* al collegamento https://www.tandfonline.com/doi/pdf/10.1080/13600834.2018.1458455, consultato da ultimo in data 21 giugno 2022).

[186] Wisconsin S.C., *State v. Loomis*, 881, N.W.2d 749 (2016) (sentenza reperibile *online* al collegamento https://www.giurisprudenzapenale.com/wp-content/uploads/2019/04/Supreme-Court-of-Wisconsin.pdf, consultato da ultimo in data 21 giugno 2022). Sul caso Loomis, *ex multis*, AA.VV., *State v. Loomis. Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing*, in *Harvard Law Review*, Vol. 130, 2017, pp. 1530 ss. (reperibile *online* al collegamento https://harvardlawreview.org/2017/03/state-v-loomis/, consultato da ultimo in data 21 giugno 2022); H. LIU – C. LIN – Y. CHEN, *Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability*, in *International Journal Of Law And Information Technology*, vol. 27, n. 2/2019, pp. 122-141 (reperibile *online* al collegamento https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313916, consultato da ultimo in data 21 giugno 2022); nella dottrina italiana, C. COSTANZI, *La matematica del processo: oltre le colonne d'Ercole della giustizia penale*, in www.questionegiustizia.it, n. 4/2018, pp. 166-188 (reperibile *online* al collegamento https://www.questionegiustizia.it/rivista/2018-4.php, consultato da ultimo in data 21 giugno 2022); S. CARRER, *Se l'*amicus curiae *è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin*, in www.giurisprudenzapenale.com, n. 4/2019 (reperibile *online* al collegamento https://www.giurisprudenzapenale.com/2019/04/24/lamicus-curiae-un-algoritmo-chiacchierato-caso-loomis-alla-corte-suprema-del-wisconsin/, consultato da ultimo in data 21 giugno 2022); M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, op. cit., pp. 5 e ss.; F. DONATI, *Intelligenza artificiale e giustizia*, op. cit., pp. 384-386; A. SIMONCINI, *Diritto costituzionale e decisioni algoritmiche*, in S. DORIGO (a cura di), *Il ragionamento giuridico*, op. cit., pp. 37-65; S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., pp. 156 e ss.

[187] Così, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 69.

[188] Cfr. Sentenza *Loomis*, cit, parr. 53-54.

[189] Tradotto: «una valutazione del rischio di COMPAS dovrebbe essere uno dei tanti fattori che vengono considerati e ponderati in sede di sentenza». Sentenza *Loomis*, cit, par. 99.

[190] Anche nei confronti del sistema HART sono state mosse delle accuse di discriminazione sulla base che, tra gli elementi alla base dell'elaborazione, vi è il codice di avviamento postale; ciò porterebbe l'algoritmo a riprodurre un

ProPublica ha sostenuto in diverse pubblicazioni che, a causa dell'opacità sull'effettivo funzionamento del dispositivo determinata dal segreto industriale, non è possibile fare alcun affidamento sui risultati prodotti; le elaborazioni, effettuate su base collettiva, non tengono conto del caso specifico; da ultimo, essendo l'algoritmo allenato con dati affetti da congeniti pregiudizi razziali, alla popolazione afro-americana risulta assegnato un fattore di rischio recidivante doppio rispetto alla popolazione bianca[191].

A queste critiche si è tentato di eccepire ricordando come in alcune circostanze, tra le quali appunto la valutazione sulla possibile recidiva del soggetto, i giudici stessi «si comportano in modo altamente automatico e in assenza di dati precisi su cui basare il loro giudizio prognostico»[192] e la discriminazione dovuta a rilevazioni di natura statistica è frequente quando è necessario sostituire l'informazione mancante con altre disponibili afferenti alla categoria cui l'individuo destinatario della decisione appartiene. Simili rilievi «non appa[iono] tuttavia sufficient[i] a giustificare l'impiego di sistemi di IA che potenzialmente possano produrre effetti discriminatori»[193]. D'altra parte, però, si è ammonito che «se tali strumenti funzionano e rispettano i diritti fondamentali, sarà difficile tenerli fuori dal perimetro della giustizia penale: già si stanno sviluppando [e imponendo] nella fase della prevenzione e in quel segmento più deformalizzato del procedimento, rappresentato dalle indagini preliminari; non v'è dubbio che si svilupperebbero anche nella fase di esecuzione»[194] (v. *infra*, per gli strumenti di polizia predittiva). Come è stato appunto osservato in riferimento a vari modelli predittivi[195], «la questione non è il rischio della sostituzione della macchina all'umano,

---

pregiudizio umano legato alle origini etniche e/o al luogo di residenza dell'individuo valutato.

[191] Cfr. J. ANGWIN – J. LARSON – S. MATTU – L. KIRCHNER, *Machine Bias*, in www.propublica.org, 23 maggio 2016 (reperibile *online* al collegamento https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, consultato da ultimo in data 21 giugno 2022); J. DRESSEL – H. FARID, *The accuracy, fairness, and limits of predicting recidivism*, in *Science Advances*, vol. 4, n. 1/2018 (reperibile *online* al collegamento https://www.science.org/doi/10.1126/sciadv.aao5580, consultato da ultimo in data 21 giugno 2022). In replica al primo studio, l'azienda produttrice di COMPAS ha risposto con un proprio scritto e, successivamente, commissionato un contro-studio, il quale avrebbe evidenziato una serie di errori nella metodica, nella misurazione e nella classificazione dei dati, commessi dai ricercatori di ProPublica: si vedano W. DIETERICH – C. MENDOZA – T. BRENNAN, *COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity*, 8 luglio 2016 (reperibile *online* al collegamento http://go.volarisgroup.com/rs/430-MBX-989/images/ProPublica_Commentary_Final_070616.pdf, consultato da ultimo in data 21 giugno 2022) e A. FLORES – K. BECHTEL – C. LOWENKAMP, *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*, vol. 80, n. 2/2016, pp. 38-46 (reperibile *online* al collegamento https://www.uscourts.gov/sites/default/files/80_2_6_0.pdf, consultato da ultimo in data 21 giugno 2022; si noti, tuttavia, che tutti e tre gli Autori di questo contro-studio fanno parte del team di ricercatori di COMPAS). Infine, come ulteriore prova della validità di COMPAS, l'azienda produttrice indica anche lo studio C. THOMPSON, *Myths and Facts: Using Risk and Need Assessments to Enhance Outcomes and Reduce Disparities in the Criminal Justice System*, NIC, marzo 2017 (reperibile *online* al collegamento https://s3.amazonaws.com/static.nicic.gov/Library/032859a.pdf, consultato da ultimo in data 21 giugno 2022).

[192] Così, J. NIEVA-FENOLL, *Intelligenza artificiale e processo*, op. cit., p. 67.

[193] In questi termini, F. DONATI, *Intelligenza artificiale e giustizia*, op. cit., p. 386.

[194] Così, M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, op. cit., p. 22.

[195] Si fa riferimento ai dispositivi di polizia predittiva, a strumenti di gestione della giustizia capaci di esprimersi sulla possibilità di archiviare il procedimento o rinviare a giudizio l'indagato e a strumenti che danno valutazioni sulla pericolosità sociale. Sugli strumenti di gestione della giustizia, si veda cfr. C. CASTELLI – D. PIANA, *Giustizia predittiva.*

ma la qualità e la scelta dei dati, la trasparenza del metodo di elaborazione degli stessi e gli scopi a cui correttamente indirizzare strumenti tecnologici sempre più potenti»[196].

Fermi i problemi sull'opacità e sull'apparente neutralità degli algoritmi e la necessità di porvi rimedio, un compromesso sull'utilizzo di tali dispositivi potrebbe essere trovato. In fin dei conti, la stessa Corte Suprema del Wisconsin ha affermato che il giudice non può fondare la propria decisione esclusivamente sull'elaborazione del COMPAS, per «la necessità che l'organo giudicante applichi i risultati del programma facendo esercizio della propria discrezionalità sulla base del bilanciamento con altri fattori»[197]. Come è stato rilevato, in questa posizione «si può riscontrare un'assonanza con gli art. 22 reg. n. 2016/679, 11 dir. n. 2016/680/UE e 8 d.lgs. n. 51 del 2018 laddove, in materia di *privacy*, vietano, in linea di massima, decisioni supportate unicamente da un trattamento automatizzato, compresa la profilazione, prescrivendo l'intervento umano nel processo decisionale automatizzato attinente alle persone fisiche»[198], se si accetta che tali prescrizioni stabiliscano che «l'*output* prodotto dall'IA va considerato come un mero indizio, che va sempre corroborato con altri elementi di prova»[199].

Se a livello giurisprudenziale pare si siano trovati dei punti di equilibrio per ritenere che, anche nei giudizi predittivi in ambito penale, l'intelligenza artificiale possa offrire un ausilio all'uomo, alle stesse soluzioni sono giunte le disposizioni eterogenee rientranti in un primo quadro di riferimento normativo predisposto per l'utilizzo dell'IA sia in ambito generale sia in campi specifici.

Il primo livello di previsioni è composto da atti di indirizzo politico, raccomandazioni di esperti e forme di *soft law*, quali le Carte etiche sopra analizzate, il *Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, con cui la Commissione europea si prefigge «il duplice obiettivo di promuovere l'adozione dell'IA e di affrontare i rischi associati a

---

La qualità della giustizia in due tempi, op. cit.; sulle valutazioni di pericolosità, brevemente, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., pp. 66-70; sull'archiviazione, R.E. KOSTORIS, *Predizione decisoria,* diversion *processuale e archiviazione*, in www.sistemapenale.it, 23 luglio 2021 (reperibile *online* al collegamento https://www.sistemapenale.it/pdf_contenuti/1627038113_kostoris-2021a.pdf, consultato da ultimo in data 21 giugno 2022).

[196] In questi termini, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 71.

[197] *Idem*, pp. 69-70.

[198] Così, G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto Penale Contemporaneo*, fasc. n. 4/2020, pp. 75-88 (reperibile *online* al collegamento https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_4_2020_Ubertis.pdf, consultato da ultimo in data 21 giugno 2022). Sulle normative citate, si veda più avanti.

[199] In questi termini, M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, op. cit., p. 17, con riferimento alle norme eurounitarie. Nel momento in cui le normative appena sopra citate vietano decisioni basate unicamente sui trattamenti automatizzati, salvo che non intervenga un uomo, non basta che quest'ultimo basi il suo provvedimento adagiandosi totalmente sull'elaborazione prodotta dal dispositivo di IA. Occorre, invece, «che l'elemento cognitivo generato dall'intelligenza artificiale sia confermato da altre fonti» (*idem*, p. 17). Analogamente, per la disposizione italiana, P. SEVERINO, *Intelligenza artificiale e diritto penale*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, op. cit., p. 544.

determinati utilizzi di questa nuova tecnologia»[200], e la Comunicazione *Promuovere un approccio europeo all'intelligenza artificiale*, una proposta di quadro normativo e un piano coordinato riveduto sull'intelligenza artificiale, che la stessa Commissione europea ha presentato con il fine di «promuovere lo sviluppo dell'IA e, allo stesso tempo, affrontare i potenziali rischi elevati che essa pone per la sicurezza e i diritti fondamentali»[201]. Lo strumento più significativo per la giustizia è rappresentato dalla citata *Carta etica europea* del 2018, mentre quello più recente è lo studio del 2020, commissionato dal Parlamento Europeo, *Artificial Intelligence and Law Enforcement. Impact on fundamental Rights*[202], che, con l'obiettivo di analizzare «*the impact on EU fundamental rights of AI in the field of law enforcement and criminal justice*»[203], focalizza l'attenzione sugli strumenti di polizia predittiva e di riconoscimento facciale, sull'utilizzo dell'intelligenza artificiale nella giustizia penale[204] e sul rapporto tra questi dispositivi e i diritti fondamentali potenzialmente violati dagli stessi[205].

Pur trattandosi di interventi di *soft law*, queste linee guida costituiscono «l'espressione di un primo indirizzo regolatore che va letto e inquadrato nell'ambito più vasto del sistema di garanzie costituito dalla CEDU e dalla normativa generale sul trattamento dei dati personali (GDPR)»[206]. Infatti, le disposizioni del GDPR possono essere utilizzate per garantire la correttezza delle decisioni assunte attraverso l'impiego di dispositivi di IA ove non sono già presenti altri principi posti a tutela, come nel caso del procedimento amministrativo. Tra le varie tutele previste dal Regolamento (UE) n. 2016/679[207], l'individuo ha il diritto di essere edotto circa «l'esistenza di un processo decisionale automatizzato, compresa la profilazione […], e, almeno in tali casi, [di ricevere] informazioni significative sulla logica utilizzata, nonché [sul]l'importanza e [sul]le conseguenze previste di tale trattamento per l'interessato» (art. 15, co. 1, let. h)); inoltre, come già

---

[200] Commissione europea, *Libro bianco sull'intelligenza artificiale*, op. cit. p. 2. Esso è espressamente condiviso dalle Conclusioni del Consiglio dell'Unione europea, *Accesso alla giustizia – Cogliere le opportunità della digitalizzazione*, in G.U.U.E., 14 ottobre 2020 n. C 342, n. 42 ss., p. I/6.

[201] Commissione europea, Comunicazione *Promuovere un approccio europeo*, op. cit., p. 1.

[202] Lo studio è presentato nel sito del Parlamento europeo (https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)656295, consultato da ultimo in data 21 giugno 2022) e commissionato precisamente dal Dipartimento tematico Diritti dei cittadini e affari costituzionali. Nello specifico, G. GONZÁLEZ FUSTER, *Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights* (PE(2020) 656295), 15 luglio 2020 (reperibile *online* al collegamento https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf, consultato da ultimo in data 21 giugno 2022).

[203] Tradotto: «l'impatto dell'IA sui diritti fondamentali dell'UE nei campi della sicurezza e della giustizia penale». *Eadem*, p. 10.

[204] Cfr. *Eadem*, pp. 21-29.

[205] Cfr. *Eadem*, pp. 37 e ss.

[206] Così, A. ZIROLDI, *Intelligenza artificiale e processo penale*, op. cit., p. 3. L'Autore si riferisce specificamente alla Carta etica prodotta dalla CEPEJ, ma lo scrivente ritiene che l'espressione possa essere riferita alla pluralità di documenti prodotti in ambito europeo sul tema.

[207] Cfr. F. DONATI, *Intelligenza artificiale e giustizia*, op. cit., p. 389-391. Per un'analisi dettagliata del rapporto tra GDPR e IA, si veda F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. PIZZETTI (a cura di), *Intelligenza artificiale*, op. cit., pp. 3-187.

segnalato, «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» (art. 22, co. 1), salvo nei casi in cui il trattamento automatizzato dei dati sia necessario per la conclusione o l'esecuzione di un contratto, sia autorizzato dal diritto dell'Unione o di uno Stato membro o si basi sul consenso esplicito dell'interessato (art. 22, co. 2, lett. a), b) e c)). In queste circostanze, all'interessato deve comunque essere riconosciuto «almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione» (co. 3).

Il secondo livello normativo, ma di diritto positivo, è invece costituito dalla Convenzione europea dei diritti dell'uomo[208], dalla Costituzione italiana e dalle disposizioni del citato Regolamento (UE) n. 2016/679 e della Direttiva (UE) n. 2016/680[209], recepita in Italia con alcune peculiarità con il D.Lgs. n. 51/2018[210]. La Direttiva è *lex specialis* rispetto al Regolamento relativo alla protezione delle persone fisiche[211], in quanto concerne specificamente la «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 e la prevenzione di minacce alla sicurezza pubblica» (art. 1, co. 1). Ne consegue che sia la sola da considerare quando si voglia capire se, quando e come strumenti di polizia predittiva e di valutazione del rischio possano essere utilizzati come ausilio all'attività dell'uomo nelle attività di prevenzione[212] e repressione penale[213]. A tal proposito, anche se la

[208] In tema, si veda S. QUATTROCOLO, *Equità del processo penale,* op. cit., che però limita la sua analisi sui profili repressivi del reato e non anche preventivi.

[209] Per un'analisi approfondita della Direttiva, si veda S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 87-103.

[210] Il Decreto regola il trattamento, interamente o parzialmente automatizzato, dei dati personali per finalità di prevenzione e repressione dei reati, esecuzione di sanzioni penali, salvaguardia e prevenzione di minacce alla pubblica sicurezza (art. 1, co. 2), stabilendo quali dati utilizzare e in che modo (artt. 3-8) e prevedendo un sistema di garanzie per l'interessato (artt. 9-12) e di responsabilità in capo alle figure chiave del titolare del trattamento (artt. 15, 16 e 20), del responsabile del trattamento (art. 18), del responsabile della protezione dati (artt. 28 e 30) e, infine, un apparato sanzionatorio (artt. 37-46).

[211] Cfr. Direttiva (UE) 2016/680, Considerando 11. Inoltre, ai sensi dell'art. 2, co. 1, lett. d) GDPR, lo stesso Regolamento non si applica ai trattamenti di dati personali «effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse». Quindi, lo scrivente non ritiene corretto che, nel trattare di dispositivi di IA utilizzati in ambito penale, parte della dottrina faccia riferimento al GDPR. Per l'applicazione del GDPR, cfr., ad esempio, C. CASTETS-RENARD – P. BESSE – J. LOUBES – L. PERRUSSEL, *Encadrement des risques techniques et juridiques des activités de police prédictive*, [Rapport de recherche] Centre des Hautes Etudes du Ministère de l'Intérieur, 2019 (reperibile *online* al collegamento https://hal.archives-ouvertes.fr/hal-02190585/document, consultato da ultimo in data 21 giugno 2022).

[212] Nel Considerando 20 della Direttiva si sottolinea che la medesima «non pregiudica la facoltà degli Stati membri di specificare le operazioni e le procedure di trattamento nelle norme nazionali di procedura penale relativamente al trattamento dei dati personali effettuato da autorità giurisdizionali e da altre autorità giudiziarie». La formula comprende quindi anche i dati trattati a fini investigativi dagli organi di polizia.

[213] Se sul piano teorico l'applicazione del Regolamento o della Direttiva sembra chiara, si riscontrano dei casi in cui la seconda va applicata anche quando il titolare del trattamento dati è diverso dalle autorità impegnate nella prevenzione e repressione penale. Si pensi all'eventualità in cui un'azienda privata faccia investigazioni interne per proprio conto (c.d. controlli difensivi, di cui si tratterà *infra*), oppure al caso di un'azienda a cui venga ordinato dalle autorità che si

Direttiva ha previsto in un'ottica di innalzamento di tutela «una medesima disciplina per il trattamento di dati personali effettuato a fini preventivi ed a fini repressivi»[214], va comunque tenuto presente che gli strumenti di polizia predittiva si pongono in una posizione particolare rispetto agli strumenti di valutazione della pericolosità adottati nelle fasi del processo sia per il momento del loro utilizzo (la regolamentazione delle attività investigative orientate a prevenire la commissione di un reato si colloca al di fuori del procedimento penale e, pertanto, nella maggior parte degli ordinamenti, è disciplinata in modo conciso) sia per il fatto che i risultati delle loro elaborazioni, almeno nel contesto italiano, non hanno dirette ricadute sulle persone, ma sono valutati dagli ufficiali delle forze di polizia per rendere più efficiente l'opera di pattugliamento e controllo del territorio e, così, impedire la commissione di certi reati (v. *infra*).

Il dato normativo, infine, è completato dalle *Linee guida WP 251* del Gruppo di lavoro articolo 29[215], che intendono meglio specificare quando sia consentita l'assunzione di una decisione fondata unicamente sul trattamento automatizzato di dati e informazioni.

Per il profilo che qui rileva maggiormente, cioè l'utilizzo di IA in ambito di prevenzione e repressione del reato, le norme che più ci interessano sono l'art. 11 Direttiva (UE) n. 2016/680 e l'art. 8 D.Lgs. 51/2018, che, pur affermando la centralità del giudice-persona e la sua insostituibilità, concedono un aggancio legislativo all'utilizzo di strumenti di intelligenza artificiale in ausilio alla sua attività[216].

L'art. 11 della Direttiva (UE) n. 2016/680 stabilisce che «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».

Se, per alcuni, tale disposizione, al pari di quella dell'art. 22 GDPR, vieterebbe in ogni caso

---

occupano di prevenzione e repressione penale di elaborare dei dati tratti in ambito commerciale per specifiche finalità investigative. Analogamente, che disciplina devono applicare i Comuni titolari dei sistemi di videosorveglianza a circuito chiuso, installati al fine di prevenzione dei reati e controllo del territorio, ai sensi dell'art. 6, cc. 7-8 D.L. 11/2009 (c.d. «Piano straordinario di controllo del territorio»)? Essendo questi sistemi di telecamere predisposti per ordinarie attività di tutela della sicurezza urbana, le regole in materia di protezione dei dati personali saranno dettate dal GDPR. Tuttavia, nel momento in cui i sistemi colgono un illecito, rilevano le disposizioni della Direttiva. Per questo motivo, nel tentativo di stabilire quando i dati vanno trattati secondo il Regolamento e quando secondo la Direttiva, i Comuni più accorti hanno già elaborato dei protocolli per affrontare situazioni al confine tra le due normative.

[214] Così, S. SIGNORATO, *Le indagini digitali*, op. cit., p. 92. L'omologazione di disciplina tra trattamenti di dati per finalità preventiva e repressiva è stata fissata anche dalla normativa italiana, a seguito dell'art. 7, D.L. 7/2015, così come modificato dalla Legge di conversione 43/2015, che ha riscritto l'art. 53 Codice Privacy.

[215] Gruppo di lavoro articolo 29 per la protezione dei dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 ed emendata il 6 febbraio 2018 (reperibile *online* al collegamento https://ec.europa.eu/newsroom/article29/items/612053, consultato da ultimo in data 21 giugno 2022).

[216] Cfr. M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, op. cit., p. 22.

di sottoporre una persona 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[217], per altri il risultato degli strumenti di valutazione del rischio potrebbe essere lecitamente ponderato dal giudice, a patto che lo stesso sia oggetto di controllo significativo (quindi, non meramente simbolico)[218] e sia considerato come mero indizio, da affiancare ad altri elementi di prova. L'intervento umano qualificato – una volta garantiti la trasparenza, l'effettivo funzionamento e la qualità dei dati in entrata – sarebbe quindi la chiave di volta per ritenere legittimo l'utilizzo di questi dispositivi nel diritto penale[219].

Allo stesso modo, nell'ambito italiano l'art. 8 del D.Lgs. 51/2018 riproduce, pur senza sovrapporsi ad esso, l'art. 22 del GDPR. Come è stato osservato, poiché «il rapporto tra GDPR e Decreto 51/2018 è di integrazione, dal momento che il Regolamento UE 679 [non si applica nei casi di trattamento di dati ai fini di prevenzione e repressione penale], la riproduzione nel decreto legislativo di una previsione analoga a quella dell'art. 22 sancisce inevitabilmente l'ingresso nel settore penale delle decisioni automatizzate»[220].

All'art. 8, co. 1 del D.Lgs. 51/2018, vista la peculiarità del contesto penale e dei diritti fondamentali della persona in gioco, sono assolutamente vietate «le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato», a meno che non «siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge». Nel caso in cui la legge le permetta, devono, dunque, essere previste garanzie adeguate per i diritti e le libertà dell'interessato, tra le quali deve essere comunque assicurato «il diritto di ottenere l'intervento umano da parte del titolare del trattamento[221]» (co. 2).

Alla luce del quadro normativo vigente, della riaffermazione di un necessario ruolo attivo dell'uomo e dei benefici che ne trarrebbe il sistema giudiziario dall'uso di dispositivi di IA, secondo alcuni[222], decisioni completamente automatizzate in campo penale potrebbero già trovare spazio nei procedimenti esecutivi promossi su istanza dell'interessato[223], e quindi destinati a produrre effetti

---

[217] Cfr. F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 22-23. L'Autore afferma che al momento, per tale motivo, «quanto meno in Europa, gli algoritmi predittivi della pericolosità criminale (e, più in generale, gli *automated decision systems* […]), non hanno avuto accesso nelle nostre aule penali».

[218] Cfr. Gruppo di lavoro articolo 29, *Linee guida sul processo decisionale*, op. cit., Sezione IV, cap. A, p. 23.

[219] In Inghilterra il *software* HART pare sia stato ammesso proprio sulla base di tale interpretazione sistematica. Cfr. Comitato sulla scienza e tecnologia della House of Common, *Algorithms in decision-making. Fourth Report of Session 2017-2019*, 23 maggio 2018, parr. 21 e 77 (reperibile *online* al collegamento https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/351/351.pdf, consultato da ultimo in data 21 giugno 2022).

[220] Così, A. ZIROLDI, *Intelligenza artificiale e processo penale*, op. cit., p. 7.

[221] Anche se non è espressamente previsto un diritto inteso alla leggibilità del procedimento algoritmico, questo può considerarsi comunque presente all'interno delle garanzie che si possono trarre nella facoltà di esigere l'intervento del giudice.

[222] Cfr. A. ZIROLDI, *ult. cit.*, p. 8.

[223] Ad esempio, nei procedimenti per *abolitio criminis* (art. 673 c.p.p.), applicazione dell'indulto (art. 672 c.p.p.) o

favorevoli (il co. 1 vieta espressamente solo le decisioni che producono effetti negativi), oppure nei procedimenti che già trovano definizione semplificata con il procedimento per decreto penale di condanna[224], nei quali dunque, proprio per esigenze di deflazione processuale, l'intervento umano è quasi standardizzato.

Tuttavia, un approccio diverso al contenuto dell'art. 11 della Direttiva e dell'art. 8 del Decreto delegato può portare l'interprete a domandarsi «se, almeno in ambito penale, le eccezioni al divieto di decisioni robotiche siano o non siano compatibili con il rispetto della dignità umana», che è quesito diverso «dal chiedersi se un algoritmo emetta o no una decisione penale corretta, dato che tale profilo sembra rilevare semmai in rapporto al diritto a un giusto processo»[225].

Se è vero che, a seguito della decisione robotica, la normativa prevede per il titolare dei dati il diritto di ottenere l'intervento umano quale garanzia inderogabile, questa precauzione non farebbe, però, venire meno il fatto della riduzione della persona ad oggetto sottoposto a giudizio matematico di una macchina, determinando così *in re ipsa* una violazione della dignità umana. Come è stato osservato, siccome «l'uomo viene reificato» dalla decisione robotica, perché ridotto ad insieme di informazioni, non si potrebbe che dedurne una chiara violazione della dignità umana: infatti, «il rispetto della dignità umana impone che l'uomo debba essere considerato e trattato sempre come persona e mai come cosa» e, di conseguenza, sia necessariamente «giudicato da un altro uomo»[226].

Data questa impostazione, ne conseguirebbe l'illegittimità degli artt. 11 Direttiva (UE) n. 2016/680 e 8 D.Lgs. 51/2018 nella parte in cui prevedono la possibilità per il diritto dell'Unione europea o degli Stati membri di autorizzare la piena e autonoma decisione robotica. In ambito penale, nell'ottica di stabilire un modello antropocentrico nel rapporto tra uomo e intelligenza artificiale, la decisione deve spettare sempre e solo all'essere umano e l'IA non può che avere un mero ruolo ancillare: infatti, dal rispetto della dignità umana si potrebbe far discendere la necessità «di riconoscere l'esistenza di un […] diritto a decisioni non basate esclusivamente su trattamenti automatizzati», da intendersi non «come mero diritto a un controllo sulla correttezza del trattamento e sulla genuinità dei dati da parte di un soggetto terzo, ma [implicante] la possibilità di un intervento umano che garantisca in ogni caso il diritto al contraddittorio sul trattamento»[227].

---

estinzione del reato.

[224] Ad esempio, nella prassi i reati di cui agli artt. 186 e 187 Codice della Strada (guida sotto l'influenza dell'alcool e in stato di alterazione psico-fisica per uso di sostanze stupefacenti) sono caratterizzati dall'automaticità dell'accertamento e da automatismi sanzionatori.

[225] In questi termini, S. SIGNORATO, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, in *Rivista di diritto processuale*, vol. 76, n. 1/2021, p. 108.

[226] *Eadem*, p. 108.

[227] Così, S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 101-102, che propone l'individuazione di tale diritto e il riconoscimento di una sua valenza costituzionale.

CAPITOLO II

PREVENZIONE E CONTROLLO

SOMMARIO: 2.1 L'utilizzo a fini preventivi dell'IA nella lotta al crimine comune ed alla corruzione. – 2.1.1 IA e sorveglianza. – 2.1.2 Digitalizzazione e IA: una nuova frontiera di contrasto alla corruzione? – 2.2 Gli strumenti di polizia predittiva. – 2.2.1 Diverse sperimentazioni, molte insidie e alcune soluzioni. – 2.2.2 La compatibilità delle attività di polizia predittiva con i principi fondamentali. – 2.2.3 Precauzioni e linee orientative in tema di polizia predittiva. – 2.3 *Big data analytics* come «baionette» contro la corruzione

2.1 L'utilizzo a fini preventivi dell'IA nella lotta al crimine comune ed alla corruzione.

Tra i fattori che insidiano la sicurezza interna degli Stati, ossia l'insieme degli organismi istituzionali e degli strumenti che tradizionalmente lo Stato adotta per tutelare il proprio apparato e i cittadini dalle minacce interne ed esterne, vi sono terrorismo[1] e criminalità comune ed organizzata, che intaccano l'ordine pubblico, la pace sociale ed il vivere democratico. La criminalità organizzata si avvale sempre più spesso anche della corruzione[2] per infiltrarsi all'interno della pubblica amministrazione ed ottenere – per il tramite, da una parte, di professionisti ed imprenditori collusi e, dall'altra, di apparati pubblici infedeli – la gestione di appalti nei settori più disparati, così da poter riciclare i proventi delle attività illecite in situazioni di apparente legalità.

Per rispondere a queste problematiche, gli Stati, anche in ottemperanza agli impegni internazionali assunti[3], hanno adottato nuove misure repressive e rafforzato l'ambito della prevenzione, aumentando le capacità operative delle forze di polizia, anche fornendo loro nuove strumentazioni tecnologiche[4], e ricorrendo, all'interno della pubblica amministrazione, a istituti, meccanismi, strumenti amministrativi e dispositivi informatici[5] per impedire il sorgere di condizioni

[1] Cfr. art. 7, cc. 1-3, L. 124/2007 (legge recante disposizioni in materia di Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto di Stato).

[2] Afferma Paola Severino, promotrice della riforma anticorruzione italiana avviata con L. 190/2012 ed eletta nel 2018 prima Rappresentante Speciale OSCE per la lotta alla corruzione, che «[la corruzione] mina la regolare attività degli apparati dello Stato, con evidenti possibili ricadute sul piano della sicurezza» (intervista del 22 maggio 2018 reperibile *online* al collegamento https://www.osce.org/it/chairmanship/454579, consultato da ultimo in data 21 giugno 2022).

[3] Ad esempio, in Italia l'adozione di una fattiva riforma di contrasto alla corruzione, introdotta con la Legge 190/2012 (Legge «Severino») recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", rispondeva anche agli obblighi derivanti dalla Convenzione ONU contro la corruzione del 31 ottobre 2003 (Convenzione di Merida) e dalla Convenzione penale sulla corruzione del Consiglio d'Europa del 27 gennaio 1999 (Convenzione di Strasburgo).

[4] In argomento, L. PASCULLI, *Genetics, robotics and crime prevention*, op. cit., pp. 187-203.

[5] Proprio nel settore della normativa antiriciclaggio opera GIANOS (Generatore Indici di Anomalia per Operazioni Sospette), un dispositivo in uso nel sistema bancario italiano per la rilevazione di operazioni finanziarie sospette, che saranno da portare a conoscenza all'Unità di informazione finanziaria (UIF) presso la Banca d'Italia. Cfr. A. ZIROLDI,

favorevoli al diffondersi della corruzione e fronteggiare casi di mala gestione della cosa pubblica.

Specificamente, vista la gran mole di dati a disposizione, le nuove tecnologie sono il mezzo su cui si è puntato su entrambi i fronti con l'obiettivo, nelle attività di polizia, di prevedere con appositi algoritmi le probabili condotte illecite e, all'interno della PA, di favorire trasparenza ed efficienza (attraverso una generale digitalizzazione) ed individuare i sintomi di una possibile condotta di corruzione in atto (grazie a specifici algoritmi). In pratica, le «tecniche in esame si inquadrano nel contesto più ampio della sorveglianza statale sugli individui per fini di sicurezza pubblica e nazionale»[6]. Aspetto questo che ha portato taluni a ragionare su questi nuovi sistemi integrati improntati sulla sorveglianza e – specie per quanto riguarda le attività di polizia – sulle ricadute che il controllo sociale per mezzo dell'analisi continua di dati eterogenei e prodotti in tempo reale può avere sulle libertà fondamentali e su temi quali la *privacy*, il rischio di discriminazione, la presunzione di innocenza[7].

Problematiche di cui gli stessi addetti ai lavori sono, peraltro, ben consci: infatti, «*while there is great potential in AI, the use of this technology by law enforcement also raises very real and serious human rights concerns that can be extremely damaging and undermine the trust communities place in law enforcement. Human rights, civil liberties and even the fundamental principles of law upon which our criminal justice system is based may be unacceptably exposed, or even irreparably compromised, if we do not navigate this route with extreme caution*»[8]. Proprio perché la sicurezza interna delle Nazioni è uno degli ambiti nei quali si sta riscontrando una

---

Intelligenza artificiale e processo penale, op. cit., p. 9. Anche se il dispositivo del caso non è direttamente utilizzato dalla PA, lo si segnala perché, pur avendo oggi gli istituti bancari natura privatistica, sono assoggettati ad importanti controlli pubblicistici, fondati sull'interesse pubblico all'attività bancaria.

[6] Così, A. BONFANTI, Big data *e polizia predittiva: riflessioni in tema di protezione del diritto alla* privacy *e dei dati personali*, in www.medialaws.eu (*Rivista di diritto dei media*), n. 3/2018, pp. 208-209 (reperibile *online* al collegamento principale https://air.unimi.it/retrieve/handle/2434/605891/1116513/bonfanti%20-%20medialaws%202018.pdf e al collegamento secondario https://www.medialaws.eu/rivista/big-data-e-polizia-predittiva-riflessioni-in-tema-di-protezione-del-diritto-alla-privacy-e-dei-dati-personali/, consultati da ultimo in data 21 giugno 2022).

[7] L'impatto di queste tecnologie sui diritti elencati è trattato oltre. Sul tema, *ex multis*, J. KREMER, *The End of Freedom in Public Places? Privacy problems arising from surveillance of the European public space*, 2017, in particolare il cap. 3.4.2, "Prediction", pp. 269-272 (reperibile *online* al collegamento https://helda.helsinki.fi/handle/10138/176300, consultato da ultimo in data 21 giugno 2022) e A. ZAVRŠNIK (a cura di), *Big Data, crime and social control*, Routledge – Taylor & Francis Group, 2018. Invece, per una prospettiva di controllo delle aziende private determinato dalle politiche commerciali, tema che non riguarda però la presente ricerca, si veda S. ZUBOFF, *Il capitalismo della sorveglianza*, Luiss University Press, Roma 2019.

[8] Tradotto: «se da un lato c'è un grande potenziale nell'IA, dall'altro l'uso di questa tecnologia da parte delle forze di polizia solleva anche preoccupazioni molto reali e serie sui diritti umani, che possono essere estremamente dannose e minare la fiducia che le comunità ripongono nelle forze di polizia. I diritti umani, le libertà civili ed anche i principi fondamentali di legge sui quali si base il nostro sistema di giustizia penale potrebbero essere inaccettabilmente esposti o anche irreparabilmente compromessi, se non intraprendiamo questo cammino con estrema cautela». INTERPOL – UNICRI, *Towards Responsible Artificial Intelligence Innovation*. *Second INTERPOL-UNICRI Report on Artificial Intelligence for Law Enforcement*, 2020, pp. 3-4 (reperibile *online* al collegamento http://www.unicri.it/towards-responsible-artificial-intelligence-innovation, consultato da ultimo in data 21 giugno 2022). Si segnala, comunque, che con il termine "*law enforcement*" ci si riferisce sia a qualunque sistema attraverso il quale soggetti individuati ed autorizzati danno applicazione alla legge in tema di sicurezza sia allo stesso personale operativo. Nella categoria di questa strumentazione rientrano, per esempio, sistemi di riconoscimento facciale e strumenti di polizia predittiva.

rapidissima implementazione dei sistemi informatici più o meno basati sull'IA, dal 2018 si tiene annualmente un incontro mondiale sul tema[9] organizzato dall'INTERPOL[10] in collaborazione con l'Istituto Interregionale delle Nazioni Unite per la Ricerca sul Crimine e la Giustizia (UNICRI[11]) per analizzare i risvolti positivi e negativi ed indicare delle linee guida etiche per il loro sviluppo.

Eppure, anche a fronte di tali rischi, è forte la convinzione di dover necessariamente ricorrere a strumenti normativi eccezionali e dispositivi informatici molto invasivi per inasprire la risposta punitiva e far così fronte alle situazioni di minaccia alla sicurezza dei cittadini e alla stabilità dell'ordinamento costituito[12]. Libertà e sicurezza, dunque, devono essere parimenti considerate e, a parere di chi scrive, messe in rapporto tra loro in maniera elastica, senza intaccare i livelli minimi di tutela irrinunciabili, al di sotto dei quali le attività di prevenzione non appaiono più proporzionate all'obiettivo, dunque tollerabili[13].

[9] Per un'analisi dei rischi e delle opportunità legati all'uso delle nuove tecnologie nell'ambito dei sistemi nazionali di sicurezza, si vedano i rapporti INTERPOL – UNICRI, *Artificial Intelligence and Robotics for Law Enforcement*, 2019 (reperibile *online* al collegamento http://www.unicri.it/index.php/artificial-intelligence-and-robotics-law-enforcement, consultato da ultimo in data 21 giugno 2022) e *Towards Responsible Artificial Intelligence Innovation*, op. cit.; anche in queste sedi non si è mancato di sottolineare la necessità che lo sviluppo e l'utilizzo di sistemi di IA siano accompagnati dall'etica e dal rispetto dei diritti umani e dei principi di correttezza, trasparenza ed esplicabilità. Infine, nel terzo rapporto è stato approfondito lo studio sui sistemi di riconoscimento facciale (la relazione è reperibile *online* al collegamento http://www.unicri.it/News/Policy-Framework-Facial-Reecognition-Law-Enforcement, consultato da ultimo in data 21 giugno 2022).

[10] The International Criminal Police Organization – INTERPOL.

[11] United Nations Interregional Crime and Justice Research Institute.

[12] Cfr., anche se limitatamente all'aspetto penale, W. NOCERINO, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Prima parte)*, in *Studium Iuris*, n. 7-8/2020, p. 821.

[13] Cfr. W. NOCERINO, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Seconda parte)*, in *Studium Iuris*, n. 9/2020, p. 1030. Sul rapporto tra prevenzione e libertà, si veda anche S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 313-317.

2.1.1 IA e sorveglianza[14]

Per quanto riguarda le attività di sorveglianza, tralasciando altre e più significative conseguenze sul sistema, come il nuovo rapporto delineatosi tra *intelligence* e forze di polizia[15] e tra

[14] «Da oggi assumo la direzione dell'ufficio politico. Voi saprete tutti che fino a ieri mi sono occupato di assassini. E con un certo successo. Non è senza significato che abbiano destinato proprio me, in questo momento, alla direzione dell'ufficio politico. Ciò è stato deciso poiché tra i reati comuni e i reati politici sempre più si assottigliano le distinzioni, che tendono addirittura a scomparire. Questo scrivetevelo bene nella memoria! Sotto ogni criminale può nascondersi un sovversivo, sotto ogni sovversivo può nascondersi un criminale. Nella città che ci è stata affidata in custodia, sovversivi e criminali hanno già steso i loro fili invisibili che spetta a noi di recidere. Che differenza passa tra una banda di rapinatori che assaltano un istituto bancario e la sovversione organizzata, istituzionalizzata, legalizzata? Nessuna! Le due azioni tendono allo stesso obiettivo, sia pure con mezzi diversi, e cioè al rovesciamento dell'attuale ordine sociale. 6.000 prostitute schedate, un aumento del 20% degli scioperi e occupazioni degli edifici pubblici e privati, 2.000 case d'appuntamento accertate, in un anno 30 attentati dimostrativi contro le proprietà dello Stato, 200 stupri in un anno, 50.000 studenti delle scuole medie in corteo per le vie della città, un aumento del 30% delle rapine e degli assalti alle banche, 10.000 schedati in più nelle file dei sovversivi, 600 omosessuali schedati, più di 70 gruppi di giovani sovversivi che agiscono al di fuori dei limiti parlamentari, un aumento del 50% delle bancarotte fraudolente e dei protesti cambiari, un numero indescrivibile di riviste politiche che invitano alla rivolta! *L'uso della libertà minaccia da tutte le parti i poteri tradizionali, le autorità costituite, l'uso della libertà che tende a fare di qualsiasi cittadino un giudice, che ci impedisce di espletare liberamente le nostre sacrosante funzioni!* Noi siamo a guardia della legge, che vogliamo immutabile! Scolpita nel tempo. *Il popolo è minorenne, la città è malata, ad altri spetta il compito di curare e di educare. A noi il dovere di reprimere!* La repressione è il nostro vaccino! *Repressione è civiltà!*» (Il «Dottore»). Dialogo tratto dal film "*Indagine su un cittadino al di sopra di ogni sospetto*", regia di Elio Petri, interpretato da Gian Maria Volonté e Florinda Bolkan, Vera Film, Roma 1970 (scena visibile *online* al collegamento https://www.youtube.com/watch?v=2h061y4h--E, consultato da ultimo in data 21 giugno 2022); corsivi miei. Il primo film italiano sulla Polizia di Stato, uscito in un contesto politico di forte crisi per lo scontro ideologico in corso nel mondo e nell'Italia repubblicana (lo scoppio della bomba nella filiale della Banca Nazionale dell'Agricoltura in piazza Fontana, a Milano, è di pochi mesi prima), voleva essere una denuncia di quelle che, per certa parte politica, erano le modalità autoritarie e prepotenti delle autorità e degli operatori delle forze di polizia nella gestione dell'ordine pubblico. Nel film sono comunque visibili, in subordine, le tematiche della sorveglianza, della raccolta di informazioni a fini preventivi, della schedatura, dell'utilizzo del «progresso» tecnologico, cioè del «regolatore» in grado di indicare i possibili legami tra un crimine e una persona «socialmente e politicamente pericolosa» già tenuta sotto controllo dalle forze di polizia (scena visibile *online* al collegamento https://www.youtube.com/watch?v=HG3HH6yXaOM, consultato da ultimo in data 21 giugno 2022); e ancóra, della possibilità di muoversi più o meno liberamente da vincoli giuridici nello svolgere le funzioni di polizia preventiva e repressiva e del ruolo che deve avere la polizia: ricadono su di lei, al pari della famiglia, della scuola e altri corpi intermedi, anche competenze educative, oppure deve occuparsi solamente dell'aspetto repressivo?

[15] Nei settori della criminalità organizzata e del terrorismo, attività d'*intelligence* e attività investigativa finiscono sempre più per condividere concetti e modalità operative. Tra l'altro, questo avvicinamento è favorito anche dall'utilizzo comune di nuovi strumenti tecnologici, pur diretti al conseguimento dei diversi obiettivi. In ambito interno, il rapporto di collaborazione tra i due comparti è stato espressamente previsto dall'art. 4, co. 3, lett. e) L. 124/2007, in forza del quale il DIS (Dipartimento delle informazioni per la sicurezza, incardinato presso la Presidenza del Consiglio dei ministri, avente il compito di coordinare le attività operative di AISI e AISE) «promuove e garantisce, anche attraverso riunioni periodiche, lo scambio informativo tra l'AISE, l'AISI e le Forze di polizia». In questo modo, si instaura un «doppio flusso osmotico» (così, W. NOCERINO, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Seconda parte)*, op. cit., p. 1023). Da una parte, «le Forze armate, le Forze di polizia, gli ufficiali e gli agenti di polizia giudiziaria e di pubblica sicurezza forniscono ogni possibile cooperazione, anche di tipo tecnico-operativo, al personale addetto ai servizi di informazione per la sicurezza, per lo svolgimento dei compiti a questi affidati» (art. 12, co. 1 L. 124/2007); inoltre, in deroga all'art. 329 c.p.p. (sul segreto degli atti d'indagine), le Agenzie di sicurezza possono acquisire gli atti d'indagine di procedimenti penali rilevanti con le loro attività (art. 118-*bis*, co. 1 c.p.p.). Dall'altra parte, l'autorità giudiziaria può acquisire documenti, atti o altre cose che si trovano presso le sedi dei Servizi di informazione per la sicurezza (art. 256-*bis*, c.p.p.), ferma la possibilità per la Presidenza del Consiglio dei ministri di confermare il segreto di Stato (art. 256-*ter*, c.p.p.); in aggiunta, i «direttori dei servizi di informazione per la sicurezza e il direttore generale del DIS hanno l'obbligo di fornire ai competenti organi di polizia giudiziaria le informazioni e gli elementi di prova relativamente a fatti configurabili come reati, di cui sia stata acquisita conoscenza nell'ambito delle strutture che da essi rispettivamente dipendono» (art. 23, co. 7 L. 124/2007).

queste ultime e le autorità giudiziarie[16], il ruolo assunto dalla *notizia criminis*[17] e l'accesso nel procedimento penale di dati e informazioni raccolti dalle agenzie di sicurezza[18], ai fini della presente trattazione preme porre maggiormente l'attenzione su due fenomeni in atto: il generale scivolamento a fini preventivi del diritto penale nel diritto amministrativo e, al suo interno, la diffusione di dispositivi di IA in ausilio alle attività di polizia[19].

Circa il primo fenomeno, si segnala che, ad imitazione del contesto legale di matrice anglosassone, anche negli ordinamenti giuridici continentali si sono imposti sistemi in cui la distinzione tra attività d'indagine (*investigating*) e attività – latamente intesa – di polizia (*policing*) si è affievolita[20]. Siccome questa attività di polizia si caratterizza per un ruolo delle forze di polizia più attivo nella gestione del fenomeno criminale ed indipendente dal controllo e dall'autorizzazione dell'Autorità giudiziaria[21], nei sistemi giuridici continentali viene normalmente tradotta con il termine "sorveglianza". In un tale sistema, infatti, ai tradizionali compiti di carattere amministrativo di garanzia dell'ordine pubblico e della sicurezza pubblica si affiancano operazioni volte al controllo sociale o che tipicamente si ritengono proprie delle Agenzie di *intelligence*[22].

Tradizionalmente, la repressione del crimine comporta la valutazione della condotta criminale e la raccolta di prove a carico del reo per provarne la colpevolezza, mentre la prevenzione ha come obiettivo quello di evitare che un crimine sia portato a compimento, interferendo nella sua

[16] La polizia è venuta acquisendo un ruolo dominante nell'attuale scenario di reazione al fenomeno terroristico e del crimine organizzato, a tutto discapito delle figure del pubblico ministero e del giudice. Tuttavia, in Italia, questo fenomeno è in parte mitigato dal ruolo di coordinamento assunto dalla Direzione Nazionale Antimafia e Antiterrorismo, alla quale sono state estese le attribuzioni in materia di delitti con finalità di terrorismo e la possibilità di avvalersi al riguardo dei servizi di polizia, così da mettere la struttura composta di magistrati al centro della rete di conoscenze scambiate tra le indagini penali e i procedimenti di prevenzione.

[17] In merito, cfr. W. NOCERINO, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Seconda parte)*, op. cit., pp. 1021-1022.

[18] Circa l'utilizzabilità processuale degli elementi raccolti dalle Agenzie di sicurezza, il procedimento penale ha perso i caratteri di impermeabilità rispetto alla fase pre-procedimentale. Verso questa direzione hanno spinto la necessità di utilizzare tutti gli strumenti di conoscenza utili e legittimi per perseguire i reati e la mancanza di un espresso divieto normativo all'acquisizione degli atti inerenti alle indagini dell'*intelligence*. Tra l'altro, il limite probatorio del segreto di Stato (art. 39, co. 1 L. 124/2007) non può essere utilizzato come argomento volto ad escludere la spendibilità processuale delle informazioni preventive d'*intelligence*, in quanto non sempre valido: infatti, le notizie relative a fatti eversivi dell'ordine costituzionale o concernenti il terrorismo, delitti di strage, associazione a delinquere di stampo mafioso e scambio elettorale politico-mafioso, non possono essere oggetto di segreto di Stato (art. 39, co. 11 L. 124/2007).

[19] Sul primo punto, approfonditamente, W. NOCERINO, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Prima parte)*, op. cit., pp. 821-827 e, della stessa Autrice, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Seconda parte)*, op. cit., pp. 1020-1031. Invece, sul secondo punto, brevemente, D. BENEDETTI, *IA e (in)sicurezza informatica*, in F. PIZZETTI (a cura di), *Intelligenza artificiale*, op. cit., pp. 253-255.

[20] Sui profili di intersezione tra prevenzione e repressione, si veda S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 318-321.

[21] Le forze di polizia di Stati Uniti d'America ed Inghilterra, per esempio, dirigono le indagini fino al momento della richiesta di rinvio a giudizio dell'indagato, mentre negli ordinamenti continentali (come in Italia, Francia, Spagna e Germania) la magistratura requirente, informata della commissione di un reato, è titolare delle indagini penali e le forze di polizia devono rispondere alle sue indicazioni e direttive.

[22] Cfr. S. QUATTROCOLO, *Equità del processo penale,* op. cit., p. 110; S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., p. 37.

pianificazione con mezzi di sorveglianza ed altre tecniche intrusive[23]. In un sistema sempre più improntato alla sorveglianza, invece, le due attività di repressione e prevenzione del crimine tendono a saldarsi e fondersi in un'unica fase di «indagini proattive»[24], caratterizzata da tecniche operative miste sia di ricerca sia di contrasto del crimine e dall'assottigliarsi sino all'indistinzione del presupposto d'avvio delle indagini preliminari, rappresentato dalla *notitia criminis*.

Anche l'ordinamento giuridico italiano, sulla spinta soprattutto dell'approvazione di atti legislativi volti al contrasto del terrorismo internazionale e del crimine organizzato, conosce da qualche anno interventi diretti «sia ad estendere l'area della punibilità e insieme ad anticiparne ulteriormente la soglia a condotte preparatorie rispetto a gravi delitti, sia ad allargare l'ambito dei poteri di controllo sociale frammisti alle indagini penali»[25]. Emblematiche in questo senso sono l'incriminazione di una serie di condotte preparatorie alla commissione di attentati terroristici[26] e la previsione di misure di prevenzione speciale *ante* o *praeter delictum*, che, di natura formalmente amministrativa, vengono emanate in condizioni di pericolosità al fine di evitare la commissione di reati, ponendosi così a cavallo tra il diritto amministrativo ed il diritto penale[27]. Dunque, la pericolosità sociale di determinati soggetti, quale indicatore della loro propensione a delinquere

[23] Nel sistema giuridico nazionale, chiara risulta la distinzione tra le funzioni di «polizia amministrativa» e «polizia giudiziaria», svolte, in presenza di determinati presupposti, dai corpi di polizia della Polizia di Stato, dell'Arma dei Carabinieri e della Guardia di Finanza; anche se le due funzioni sono spesso svolte dai medesimi soggetti, la prima è diretta dal Ministero dell'Interno (localmente, a sensi degli artt. 13 e 14, L. 121/1981, la competenza spetta a prefetto e questore), mentre la seconda dal pubblico ministero (art. 56, c.p.p.). La polizia amministrativa si occupa dell'osservanza della legge e dei regolamenti amministrativi, in esecuzione delle funzioni proprie del potere esecutivo. La polizia amministrativa si suddivide in specializzazioni, quali, ad esempio, la polizia tributaria, la polizia sanitaria e la polizia di sicurezza. Proprio la polizia di sicurezza, ai sensi dell'art. 1, R.D. 773/1931 (Testo Unico delle leggi di pubblica sicurezza), è specificamente chiamata ad occuparsi di ordine pubblico e pubblica sicurezza, garantendo le condizioni di pace sociale, prevenendo i fattori che la minacciano ed eliminando gli stati di turbativa già in atto. Invece, la polizia giudiziaria, per come regolata all'art. 55, c.p.p., «deve, anche di propria iniziativa, prendere notizia dei reati, impedire che vengano portati a conseguenze ulteriori, ricercarne gli autori, compiere gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale».

[24] Tale termine si è diffuso con la Risoluzione del XVIII Congresso Internazionale di Diritto Penale, Istanbul, 20-27 settembre 2009, ove si afferma al Punto 9 che «Oggetto delle indagini proattive è l'accertamento degli *interna corporis* delle associazioni dedite alla sistematica commissione di reati o al terrorismo. Tali indagini sono finalizzate a prevenire la preparazione e la commissione di detti reati così come al reperimento di indizi utili per avviare indagini penali contro quelle associazioni e/o contro i loro membri». Per un primo commento sulla Risoluzione e la relativa traduzione si veda R.E. KOSTORIS, *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella Risoluzione del XVIII Congresso internazionale di diritto penale*, in *Rivista di Diritto Processuale*, n. 2/2010, pp. 327 e ss.; il Punto 9 è riportato a p. 335.

[25] Così, D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Archivio Penale*, n. 1/2016, p. 44.

[26] Tra le quali il reclutamento, l'addestramento, il trasporto, il finanziamento o la fornitura di equipaggiamento a soggetti che si spostano verso Stati diversi da quelli di propria nazionalità, mossi dal fine di commettere, organizzare o partecipare ad atti di terrorismo (vedi artt. 270-*quater* e ss., c.p.).

[27] Nel contesto italiano, la normativa di riferimento per le misure di prevenzione è il D.Lgs. 159/2011 (Codice delle leggi antimafia e delle misure di prevenzione), ma previsioni ulteriori si rinvengono nella legislazione speciale. Le misure di prevenzione non vanno confuse con le misure amministrative di sicurezza, di cui agli artt. 199 e ss., c.p., che afferiscono al momento successivo del processo penale e si applicano a persone socialmente pericolose che abbiano commesso un reato ed è ritenuto probabile ne commettano di nuovi. Per un'analisi delle misure di prevenzione, si veda Corte EDU, sentenza de Tommaso c. Italia (ricorso n. 43395/09), 23 febbraio 2017 (sentenza reperibile *online* al collegamento https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-171804%22]} , consultato da ultimo in data 21 giugno 2022).

evincibile da un giudizio prognostico, dovrebbe fungere da fattore di rischio predittivo della possibile commissione o reiterazione di illeciti da parte di un soggetto determinato.

Di conseguenza, tolta «o annebbiata che sia la cornice formale degli istituti giuridici, a divenire sfuggenti sono le stesse coordinate della verifica di proporzionalità sulle misure destinate ad incidere nella sfera dei diritti fondamentali: non è circoscritta a priori la platea di individui potenziali soggetti passivi; resta dubbio lo scopo dell'intrusione; si sottrae a solide geometrie scalari la relazione tra gravità del fatto temuto o commesso, livello dei requisiti necessari all'intervento reattivo dell'autorità e importanza del bene del singolo sottoposto a limitazione. Ne deriva l'estrema elasticità dei bilanciamenti, il che equivale a rendere flessibili verso il basso le garanzie individuali»[28].

Venendo al secondo aspetto (l'impiego dell'IA quale ausilio delle attività di polizia), questo fenomeno di assottigliamento tra le attività di *intelligence* e di polizia amministrativa/giudiziaria ha comportato nella lotta al crimine un'estensione dei compiti delle forze di polizia, che, a cominciare dall'area della pubblica sicurezza, hanno aumentato l'attività di raccolta occulta di informazioni per mezzo di metodi tradizionali e di «indagini digitali»[29]. L'operazione di provvista del secondo tipo avviene sia in un momento non coperto dalle garanzie del procedimento penale, per mezzo di strumenti informatici di controllo del territorio[30] ed algoritmi capaci di raccogliere dati eterogenei ed estrarne informazioni (*data mining*), sia durante il procedimento, attraverso vari dispositivi tecnologici, tra i quali spicca il captatore informatico[31], o *trojan*, una sorta di *virus* o *malware* che,

[28] Così, D. NEGRI, *ult. cit.*, p. 46.

[29] «Con la locuzione "indagini digitali" si può indicare qualunque tipologia investigativa che impieghi la tecnologia digitale, indipendentemente dal tipo di reato perseguito, che potrebbe essere sia informatico, sia cibernetico, sia comune». Così, S. SIGNORATO, *Le indagini digitali*, op. cit., p. 44. Le indagini digitali non vanno confuse con le indagini informatiche, che sono invece finalizzate ad individuare elementi in formato digitale in grado di assumere valore probatorio rispetto ad un crimine informatico, come lo spionaggio e l'hackeraggio.

[30] Tra questi vi rientrano, per esempio, quei programmi capaci di identificare un soggetto a partire da un fotogramma, confrontando lo stesso con i dati già in possesso alle forze di polizia o con le telecamere di sorveglianza di una determinata zona. Nel contesto italiano, un *software* di questo tipo utilizzato dalla Polizia di Stato è il SARI (Sistema Automatico di Riconoscimento Immagini). Per una breve panoramica dei sistemi di IA utilizzati dalle forze di polizia italiane, si veda V. GUARRIELLO, *I sistemi di intelligenza artificiale in uso alle Forze dell'Ordine in Italia*, in www.salvisjuribus.it, 10 maggio 2020 (reperibile *online* al collegamento http://www.salvisjuribus.it/i-sistemi-di-intelligenza-artificiale-in-uso-alle-forze-dellordine-in-italia/, consultato da ultimo in data 21 giugno 2022).

[31] Il captatore informatico rientra tra la strumentazione digitale a disposizione delle forze di polizia e delle autorità coinvolte nell'ambito del procedimento penale per perseguire le fattispecie di reato per le quali la legge ne prevede espressamente l'uso. Allo scrivente, però, non risulta che questa tecnologia sia stata dotata di una qualche capacità autonoma di rielaborazione dei dati raccolti che la possa far rientrare nella categoria di IA qui considerata e, per questo motivo, non sarà oggetto di approfondimento. Tuttavia, viste l'importanza che il captatore riveste nel campo repressivo, le continue rimodulazioni normative a cui è stato sottoposto negli ultimi anni, e l'ammissibilità del suo utilizzo per le indagini nei reati di corruzione, in merito si vedano, *ex multis*, G. LASAGNI, *L'uso di captatori informatici (*trojans*) nelle intercettazioni tra presenti*, in *Diritto Penale Contemporaneo*, 7 ottobre 2016 (reperibile *online* al collegamento https://www.penalecontemporaneo.it/upload/LASAGNI_2016b.pdf, consultato da ultimo in data 21 giugno 2022); C. PINELLI, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di Stato"*, in *Diritto Penale Contemporaneo*, fasc. n. 4/2017 (reperibile *online* al collegamento https://archiviodpc.dirittopenaleuomo.org/upload/2925-pinelli417.pdf, consultato da ultimo in data 21 giugno 2022); S. SIGNORATO, *Modalità procedimentali dell'intercettazione tramite captatore informatico*, in G. GIOSTRA – R. ORLANDI

inoculato segretamente all'interno di qualunque dispositivo informatico ed attivato, può effettuare plurime attività.

L'irrompere di nuove tecnologie di sorveglianza in funzione investigativa si deve allo «spostamento dell'asse delle indagini penali dalla tradizionale sfera della repressione verso quella della prevenzione» per esigenze di contrasto a gravi fenomeni criminosi; necessità che comportano, appunto, «un sensibile rafforzamento dei poteri di controllo della collettività e, conseguentemente, un più intenso ricorso a modalità occulte di raccolta delle informazioni attraverso l'uso di nuovi ed invasivi strumenti di sorveglianza»[32].

Sulla possibilità di utilizzare strumentazione intrusiva anche in una fase senza guarentigie procedimentali, si precisa subito quanto segue. L'attività di polizia di sicurezza, «*for reasons of effectiveness*»[33], è molto meno regolata dalla legge rispetto al momento delle indagini preliminari, ove invece sono imposti rigorosi criteri di acquisizione di informazioni e della prova, perché, se fosse diversamente, ne risulterebbe leso l'aspetto di concreta individuazione di soggetti che stanno per commettere un reato. A ben vedere, gli stessi trattati internazionali che affermano diritti e libertà in ambito penale tendono a fare esplicito riferimento al procedimento penale e non alla fase di prevenzione, con la conseguenza che in quest'ultima le garanzie previste per gli indagati – le quali si traducono in vincoli per le autorità – non si applicano[34]. Tra le varie tecniche di prevenzione, anche lo «sfruttamento di un'eventuale i.a. in questo ambito non trova, pertanto, un limite delineato da disposizioni procedurali, quanto [– come si vedrà –] di selezione delle "fonti" di dati e

---

(a cura di), *Nuove norme in tema di intercettazioni*, Giappichelli Editore, Torino 2018, pp. 263-275; S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 299-302; O. CALAVITA, *L'odissea del* Trojan Horse, in *Diritto Penale Contemporaneo*, fasc. n. 11/2018 (reperibile *online* al collegamento https://archiviodpc.dirittopenaleuomo.org/upload/3575-calavita2018a.pdf, consultato da ultimo in data 21 giugno 2022); M. BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in *Diritto Penale Contemporaneo*, 20 dicembre 2018 (reperibile *online* al collegamento https://www.penalecontemporaneo.it/upload/6629-bontempelli2018a-converted.pdf, consultato da ultimo in data 21 giugno 2022); S. SIGNORATO, *Intercettazioni di comunicazioni*, in R. ORLANDI – S. SEMINARA (a cura di), *Una nuova legge contro la corruzione*, Giappichelli Editore, Torino 2019, pp. 245-260; L. CAMALDO, *Le innovazioni previste dalla legge anticorruzione in tema di intercettazioni con captatore informatico*, in *Diritto Penale Contemporaneo*, 24 settembre 2019 (reperibile *online* al collegamento https://archiviodpc.dirittopenaleuomo.org/upload/6132-camaldo2019a-converted.pdf, consultato da ultimo in data 21 giugno 2022); G. CANESCHI, *Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2019, pp. 417-429 (reperibile *online* al collegamento https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_caneschi.pdf, consultato da ultimo in data 21 giugno 2022); M. GRIFFO, *Il* trojan *e le derive del terzo binario*, in *Sistema penale*, n. 2/2020, pp. 61-70; L. GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *Sistema penale*, n. 4/2020, pp. 109-143; A. PROCACCINO – W. NOCERINO, *Le nuove investigazioni nei reati corruttivi informatici*, in *Diritto penale e processo*, n. 12/2020, pp. 1623-1640; S. SIGNORATO, *Rimodulazioni normative dell'uso investigativo del captatore informatico*, in R. ORLANDI – G. GIOSTRA (a cura di), *Revisioni normative in tema di intercettazioni. Riservatezza, garanzie difensive e nuove tecnologie informatiche*, Giappichelli Editore, Torino 2021, pp. 319-335.

[32] Così, F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2018, p. 177 (reperibile *online* al collegamento https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/nicolicchia.pdf, consultato da ultimo in data 21 giugno 2022).

[33] Tradotto: «per ragioni di efficacia». S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., p. 38.

[34] Cfr. *Eadem*, p. 38.

informazioni che possono essere utilizzati»[35] per questo fine e di rispetto di alcuni principi fondamentali.

2.1.2 Digitalizzazione e IA: una nuova frontiera di contrasto alla corruzione?[36]

Per quanto riguarda lo specifico ambito anticorruzione, rilevano sia una maggior correlazione tra i settori amministrativo e penale sia la volontà di utilizzare la tecnologia per contrastare il fenomeno criminale *de qua*, garantendo la trasparenza attraverso una generale digitalizzazione[37] e, tramite l'ausilio di specifici algoritmi, monitorare il sorgere del rischio corruzione[38].

Nell'utilizzo della digitalizzazione e di specifici algoritmi anticorruzione è possibile riscontrare due approcci: quello dall'alto corrisponde alla tradizionale imposizione da parte del potere pubblico di leggi, regolamenti e procedure all'interno della PA volte a prevenire il rischio corruzione; quello dal basso, invece, fa affidamento sui valori della società civile e sulla volontà della comunità di segnalare situazioni di anomalia. L'intelligenza artificiale può assistere entrambi gli approcci, come dimostrano, per esempio, i casi dei programmi KALSADA e Zero Trust e delle piattaforme ucraine ProZorro e Dozorro.

Nelle Filippine è stato adottato un approccio dall'alto verso il basso con il programma KALSADA, che valuta la qualità dei materiali da costruzione stradale e, di conseguenza, identifica potenziali casi di corruzione e appropriazione indebita, nel caso in cui le opere non siano realizzate nei tempi ed ai prezzi previsti o siano utilizzati materiali scadenti, in frode ai contratti stipulati con le autorità pubbliche. Sempre in un'ottica dall'alto, in Cina dal 2012 è stato sviluppato Zero Trust, un *software* di IA in grado di scovare segni di corruzione a livello istituzionale attraverso l'incrocio di dati tratti dalle banche, dai registri delle proprietà e dai satelliti; segnalando movimenti bancari sospetti o il possesso di beni non dichiarati, il sistema comunica al personale quali dipendenti

[35] In questi termini, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 56.

[36] «In un paese corrotto o si è corruttori o si è fessi» (Enrico Mattei).

[37] Ad esempio, il Consiglio dei Ministri OSCE ha adottato una decisione sulla lotta alla corruzione che, tra l'altro, ribadisce l'impegno degli Stati a rafforzare la trasparenza e la gestione dei sistemi dei bandi di gara per opere e servizi, anche attraverso l'utilizzo della digitalizzazione e garantendo l'accessibilità alle risorse *online* della pubblica amministrazione. OSCE, *Prevenzione e lotta alla corruzione attraverso la digitalizzazione e una maggiore trasparenza*, decisione n. 6/20, Tirana, 2020 (reperibile *online* al collegamento https://www.osce.org/files/f/documents/4/e/479801.pdf, consultato da ultimo in data 21 giugno 2022; il testo *Preventing and Combating Corruption Through Digitalization and Increased Transparency*, in lingua originale inglese, è invece reperibile *online* al collegamento https://www.osce.org/files/f/documents/3/7/479759.pdf, consultato da ultimo in data 21 giugno 2022). Sull'impiego di strumentazione tecnologica e la digitalizzazione, cfr. Punti 1.b) e 1.c).

[38] Sull'utilizzo di specifici algoritmi anticorruzione, cfr. OSCE, *ult. cit.*, Punto 1.d): gli Stati partecipanti prevengono e combattono la corruzione «promuovendo l'uso di strumenti digitali per l'individuazione precoce e la prevenzione della corruzione».

pubblici potrebbero essersi comportati in modo infedele[39].

Invece, in Ucraina si è assistito ad un approccio dal basso. Il sistema ProZorro (dall'ucraino, "trasparente") è stato creato grazie all'iniziativa congiunta di volontari, aziende e Ministero dell'Economia ucraino, col fine di rendere le procedure per i bandi di gara più trasparenti e libere da condizionamenti esterni. Visti i risparmi di spesa ed i guadagni in termini di efficacia ed efficienza delle procedure amministrative ottenuti in fase di sperimentazione, dal 2016 gli operatori pubblici devono pubblicare nel portale tutte le notizie riguardanti gli appalti e i prestatori di servizi possono presentare le proprie proposte attraverso il modulo delle aste *online*[40]. Nella stessa ottica di controllo dal basso, il portale di monitoraggio Dozorro, creato da Transparency International Ukraine, permette ai partecipanti al sistema (fornitore, cliente, ente di controllo, cittadino), tra le altre cose, di discutere e valutare le condizioni di un particolare appalto, di analizzare gli appalti di una particolare agenzia governativa o istituzione, segnalare possibili irregolarità, preparare e presentare ricorso ufficiale alle autorità di regolamentazione[41]; in tutto ciò, il portale attinge all'IA per indicare gli appalti pubblici ad alto rischio di corruzione alle autorità, che così possono sorvegliare l'andamento e la regolarità della procedura e l'effettiva realizzazione delle prestazioni pattuite.

In pratica, invece del governo «*taking the role of big brother watching over the citizens, AI-ACT, in particular when used by bottom-up efforts, allow the public to turn into many little watchdogs keeping the government in check*»[42].

Anche in Italia la prevenzione ha rappresentato la chiave di volta della nuova strategia di lotta alla corruzione (allargata anche alla mala amministrazione) inaugurata con la L. 190/2012: infatti, da quel momento è stato declinato un sistema integrato che affianca alla «leva tradizionale» composta da misure repressive di carattere penale una «leva nuova» fatta di misure preventive di carattere amministrativo. I pilastri del nuovo sistema improntato sulla prevenzione sono diventati,

---

[39] Cfr. cfr. S. CHEN, *Is China's corruption-busting AI system "Zero Trust" being turned off for being too efficient?*, in *South China Morning Post*, 4 febbraio 2019, reperibile *online* al collegamento https://www.scmp.com/news/china/science/article/2184857/chinas-corruption-busting-ai-system-zero-trust-being-turned-being, consultato da ultimo in data 21 giugno 2022).

[40] Cfr. sito istituzionale https://prozorro.gov.ua/en, consultato da ultimo in data 21 giugno 2022. In pratica, si tratta di quella digitalizzazione delle procedure per l'assegnazione di opere e servizi (*e-procurement*) che per il contesto italiano è stabilita dall'art. 44 del Codice dei contratti pubblici.

[41] Cfr. sito ufficiale https://dozorro.org/, consultato da ultimo in data 21 giugno 2022.

[42] Tradotto: «che assume il ruolo di Grande fratello che veglia sui cittadini, gli AI-ACT, in particolare se utilizzati con approcci dal basso verso l'alto, consentono al pubblico di trasformarsi in tanti piccoli cani da guardia che tengono sotto controllo il governo». N. KÖBIS – C. STARKE – I. RAHWAN, *Artificial Intelligence as an Anti-Corruption Tool (AI-ACT). Potentials and Pitfalls for Top-down and Bottom-up Approaches*, in www.arxiv.org, Sez. *Computer Science > Computers and Society*, 23 febbraio 2021, p. 7 (reperibile *online* al collegamento https://arxiv.org/ftp/arxiv/papers/2102/2102.11567.pdf, consultato da ultimo in data 21 giugno 2022). Per AI-ACT si intende "*AI-based anti-corruption tools*", cioè strumenti anticorruzione basati sull'IA.

tra i tanti, la trasparenza[43], gli obblighi di pubblicazione, l'inconferibilità/incompatibilità di incarichi, i conflitti di interesse, la stesura di piani di prevenzione della corruzione e la previsione di codici di comportamento, la vigilanza sugli appalti e, infine, la semplificazione[44] e la digitalizzazione. Nell'ottica di utilizzare l'organizzazione amministrativa stessa per prevenire i fenomeni corruttivi, «la filosofia di fondo è stata quella di coinvolgere i funzionari pubblici in un approccio proattivo alla lotta alla corruzione, costruendo quei meccanismi di gestione che possano consentire di operare individuando il rischio e predisponendo cautele dirette a minimizzarlo»[45].

Tra le prime misure con finalità anticorruzione – quanto meno, qui intesa in senso lato – vi sono stati gli obblighi di pubblicazione concernenti i contratti pubblici, volti a favorire la trasparenza delle procedure di acquisto, previsti dal combinato disposto degli artt. 37 Decreto «Trasparenza» (D.Lgs. 33/2013) e 29 Codice dei contratti pubblici (D.Lgs. 50/2016)[46]. «In questo senso, la digitalizzazione, in quanto volta a favorire forme di controllo diffuso sul corretto utilizzo delle risorse pubbliche, può essere considerata anche come misura di prevenzione della corruzione»[47].

Al giorno d'oggi, sia le pubbliche amministrazioni che le imprese private hanno puntato

---

[43] Come statuisce lo stesso Decreto «Trasparenza» (D.Lgs. 33/2013), la «trasparenza è intesa come accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche» (art. 1, co. 1).

[44] I Decreti «Sblocca-Cantieri», «Semplificazioni» e «Semplificazioni *bis*» (rispettivamente nn. 32/2019, 76/2020 e 77/2021) hanno introdotto misure di semplificazione nel Codice Appalti, principalmente attraverso un notevole ampliamento degli affidamenti senza gara e la possibilità di nominare commissari straordinari per la realizzazione di opere complesse. Sul punto, cfr. C. BENETAZZO, *Gli appalti pubblici nel PNRR tra semplificazione e prevenzione della corruzione*, in www.federalismi.it, n. 29/2021, pp. 128-129 (reperibile *online* al collegamento https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=46473&dpath=document&dfile=28122021233147.pdf&content=Gli%2Bappalti%2Bpubblici%2Bnel%2BPNRR%2Btra%2Bsemplificazione%2Be%2Bprevenzione%2Bdella%2Bcorruzione%2B%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B, consultato da ultimo in data 21 giugno 2022). La stessa Autorità azionale anticorruzione (ANAC) si era pronunciata sugli interventi governativi introdotti con il Decreto «Semplificazioni» esprimendo giudizi positivi e critici per le varie misure adottate; cfr. ANAC, *Esame e commento degli articoli del decreto-legge 16 luglio 2020, n. 76 «Misure urgenti per la semplificazione e l'innovazione digitale» in tema di contratti pubblici, trasparenza e anticorruzione*, 4 agosto 2020 (reperibile *online* al collegamento https://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/Pubblicazioni/RapportiStudi/ContrattiPubblici/Anac.DL76.2020.pdf, consultato da ultimo in data 21 giugno 2022).

[45] Così, A. GULLO, *Note minime sul rapporto tra diritto amministrativo e diritto penale*, in *Luiss Law Review*, n. 2/2018, p. 39 (reperibile *online* al collegamento https://lawreview.luiss.it/files/2015/11/NUMERO-2-2018-1.pdf, consultato da ultimo in data 21 giugno 2022).

[46] All'art. 29 D.Lgs. 50/2016, rubricato «Principi in materia di trasparenza», si deve l'introduzione di nuovi obblighi di pubblicazione che si sono aggiunti a quelli previsti dall'art. 1, co. 32 L. 190/2012, con la previsione della pubblicazione
nella sezione "Amministrazione trasparente" di «tutti gli atti delle amministrazioni aggiudicatrici e degli enti aggiudicatori relativi alle procedure per l'affidamento di appalti pubblici di servizi, forniture, lavori e opere, di concorsi pubblici di progettazione, di concorsi di idee e di concessioni». Non avendo, però, la norma chiarito quali fossero realmente gli atti da pubblicare nel rispetto del D.Lgs. 33/2013, l'ANAC, con la delibera n. 1310/2016, ha individuato gli atti oggetto di pubblicazione, tra cui figurano gli avvisi di preinformazione, i bandi e gli avvisi di gara, la delibera a contrarre, l'elenco degli atti relativi ad affidamenti diretti o affidamenti *in house*, compresi i provvedimenti di esclusione o di ammissione nonché l'elenco dei verbali di gara. Tuttavia, si fa presente che rimane la distinzione tra pubblicità di atti con mera finalità di trasparenza e pubblicità di atti con produzione di effetti legali.

[47] Così, C. BENETAZZO, *Intelligenza artificiale e nuove forme di interazione*, op. cit., p. 31.

sull'utilizzo delle nuove tecnologie per gestire la gran mole di dati eterogenei (*big data*) con cui entrano in contatto e trarne altre utili indicazioni: come era già stato osservato dall'Agenzia per l'Italia Digitale (AgID)[48], preposta alla promozione dell'innovazione digitale del Paese, pur «rappresentando una miniera di informazioni, i dati hanno bisogno di strumenti adeguati per poter essere sfruttati in tutto il loro potenziale. In particolare, servono modelli e metodi di recupero e filtraggio delle informazioni fondati su tecnologie semantiche e ontologie condivise»[49].

Tra le varie finalità a cui volgere l'elaborazione di questo flusso di materiale, specie nel sistema anglosassone, «i recenti sviluppi della prassi in materia dimostrano che esiste la possibilità di trasformare dati asettici in informazioni rilevanti per la prevenzione del rischio corruzione»[50], grazie a sistemi automatizzati che lo valutano e propongono delle procedure per gestirlo.

Requisito essenziale affinché l'IA possa operare con fini di anticorruzione è, però, la presenza di un sistema amministrativo fondato sulla digitalizzazione e capace di mettere in comunicazione tra loro le diverse piattaforme digitali su cui le diverse articolazioni amministrative operano e portano avanti i vari procedimenti di competenza[51].

Per quanto riguarda il contesto italiano, nell'ottica di raggiungere questo obiettivo base e favorire quindi l'interoperabilità[52] dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici, con il PNRR e gli interventi legislativi di attuazione si è puntato al superamento delle illogiche frammentazioni di competenza per la digitalizzazione della PA e alla rivisitazione di tutta una serie di progetti già avviati, ma che si trovavano in una situazione di stallo o avevano portato a risultati deludenti. Ciò con l'intento di

---

[48] L'AgID, sottoposta ai poteri di indirizzo e vigilanza del Presidente del Consiglio dei ministri o del ministro da lui delegato, è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e coordinare le amministrazioni nel percorso di attuazione del *Piano triennale per l'informatica della pubblica amministrazione*, favorendo la trasformazione digitale del Paese.

[49] Task Force IA dell'AgID, *Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino*, 2018, p. 52 (reperibile *online* al collegamento https://ia.italia.it/assets/librobianco.pdf, consultato da ultimo in data 21 giugno 2022). Si tratta del primo documento indirizzato alle amministrazioni pubbliche – scuole, strutture sanitarie, Comuni, Tribunali, Ministeri – che contiene raccomandazioni e indicazioni su come sfruttare al meglio le opportunità offerte dall'intelligenza artificiale, limitandone criticità e aspetti problematici, per sviluppare servizi pubblici sempre più a misura di cittadino. Per un commento sul documento dell'AgID, si veda M. TRESCA, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia digitale*, in www.medialaws.eu (*Rivista di diritto dei media*), n. 3/2018, pp. 240-252 (reperibile *online* al collegamento https://ia.italia.it/assets/tresca.pdf, consultato da ultimo in data 21 giugno 2022).

[50] In questi termini, E. BIRRITTERI, Big Data Analytics *e* compliance *anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2019, p. 290 (reperibile *online* al collegamento https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_biritteri.pdf, consultato da ultimo in data 21 giugno 2022).

[51] Per una panoramica sullo stato della digitalizzazione del Paese pre crisi pandemica e PNRR e sulle implicazioni derivanti sui diritti dei singoli nell'ambito del rapporto con i pubblici poteri, cfr. M. CAPORALE, *Dalle* smart cities *alla cittadinanza digitale*, in www.federalismi.it, n. 2/2020, pp. 29-46 (reperibile *online* al collegamento https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=40901&dpath=document&dfile=22012020144617.pdf&content=Dalle%2Bsmart%2Bcities%2Balla%2Bcittadinanza%2Bdigitale%2B%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B, consultato da ultimo in data 21 giugno 2022).

[52] Per interoperabilità si intende la capacità di un sistema di cooperare e di scambiare informazioni o servizi con altri sistemi in modo corretto, completo, affidabile e privo di errori.

superare la farraginosità che tradizionalmente caratterizza il sistema amministrativo interno e (anche) così dare impulso alla ripresa economica dopo la crisi dovuta dalla pandemia di COVID-19: infatti, lo stato generale di incompiutezza di centinaia di grandi opere in Italia «[n]on è solo un problema di coperture finanziarie ma anche di procedure amministrative spesso oscure e farraginose, di cui sono prime vittime i cittadini e le imprese ma che poi finiscono per soffocare la stessa amministrazione, vittima a sua volta di una legislazione interpretazione ipertrofica, che neanche davanti ai giudici trova univoca interpretazione»[53]. Ecco, dunque, «che la vera partita per l'innovazione e la crescita economica del Paese si gioca sulla capacità di condividere e riutilizzare i dati, valorizzando il patrimonio informativo della Pubblica Amministrazione»[54].

Vista la competenza esclusiva statale in materia di «coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale» (art. 117, co. 2, lett. r) Cost.), con l'occasione, sono state anche ridelineate le competenze in materia di digitalizzazione[55] in capo al Ministero per l'innovazione tecnologica e la transizione digitale – Dipartimento per la trasformazione digitale e all'AgID per far fronte sia alle sfide di rinnovamento contenute nel PNRR sia agli obblighi di legge contenuti nei nuovi testi normativi europei in materia di digitalizzazione, quali il Regolamento UE n. 2018/1724 sullo Sportello unico digitale europeo (*Single Digital Gateway*)[56] e la Direttiva UE n. 2019/1024 sull'apertura dei dati e sul riutilizzo dell'informazione del settore pubblico, attuata in Italia con il D.Lgs. 200/2021[57].

Tra l'altro, la centralizzazione delle politiche relative alla implementazione dei presupposti necessari alla definizione di una cittadinanza digitale può essere implicitamente presupposta anche dall'art. 117, co. 2, lett. m), della Costituzione, lì dove si fa riferimento alla «determinazione dei

---

[53] Così, C. BENETAZZO, *Gli appalti pubblici nel PNRR*, op. cit., p. 127. Sull'ipertrofia normativa che caratterizza il sistema degli appalti in Italia, si veda C. BENETAZZO, *ANAC e sistema europeo dei contratti pubblici*, Giappichelli Editore, Torino 2020, pp. 1-31 (*Introduzione*). D'altronde, il dilagare della corruzione con l'aumentare della produzione normativa e della burocratizzazione è un fenomeno antico, se già Publio Cornelio Tacito, nel I secolo d.C., affermava che «*corruptissima re publica plurimae leges*» (tradotto: «nella somma corruzione della cosa pubblica, infinito il numero delle leggi») (*Annales*, Libro III, par. 27).

[54] In questi termini, I. MACRÌ, Open data, open format: *trasparenza e pubblicità dei dati delle Pubbliche Amministrazioni*, in *Azienditalia*, n. 8-9/2021, p. 1438.

[55] Fino a questo momento, la digitalizzazione dell'amministrazione era stata abbastanza trascurata e non accuratamente delegata al Ministero per la Pubblica Amministrazione – Dipartimento per la Funzione pubblica.

[56] Lo Sportello Digitale Unico vuole offrire ai cittadini e alle imprese europee un facile accesso a informazioni di alta qualità e procedure *online* efficienti e armonizzate basate sul principio *once only*, secondo il quale non si dovranno più fornire le informazioni di cui la PA è già in possesso. La semplificazione e la riduzione dell'onere amministrativo non possono prescindere, infatti, dalla condivisione "una volta per tutte" e in modo immediato ed efficace, delle informazioni della Pubblica Amministrazione, attualmente detenute in modo frammentario tra molteplici enti. Il Regolamento pare anche delineare una struttura embrionale di procedimento amministrativo digitale. Sul punto, si veda il collegamento *online* https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2022/02/21/pa-digitale-2026-i-progetti-sportello-digitale-unico-accessibilita-entrano-vivo, consultato da ultimo in data 21 giugno 2022.

[57] Va anche segnalata la Comunicazione *Quadro europeo di interoperabilità* (COM(2017) 134 final, Brussels, 23.3.2017) della Commissione europea, con la quale sono state gettate le basi per l'armonizzazione di alcuni procedimenti principali (reperibile *online* al collegamento https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0012.02/DOC_2&format=PDF, consultato da ultimo in data 21 giugno 2022).

livelli essenziali delle prestazioni concernenti i diritti civili e politici che devono essere garantiti su tutto il territorio nazionale». Quando si parla di cittadinanza digitale e azione della pubblica amministrazione, si evocano senz'altro diritti individuali, civili e politici, che si proiettano nella sfera pubblica e richiedono prestazioni da parte del pubblico potere per essere soddisfatti.

L'individuazione delle banche dati di interesse nazionale, la loro armonizzazione e la pianificazione delle attività per garantirne l'accesso sono state oggetto di considerazione negli interventi legislativi e nelle varie linee guida di attuazione del PNRR che recentemente hanno interessato la materia della gestione del patrimonio informativo pubblico per fini istituzionali: ci si riferisce, in particolare, al D.L. «Semplificazioni»[58] e D.L. «Semplificazioni *bis*»[59], al *Piano triennale per l'informatica nella pubblica amministrazione 2020-2022*[60] e all'*Agenda Semplificazione 2020*[61].

Tra i vari interventi previsti, vi è anche il superamento della fase di sperimentazione della Piattaforma Digitale Nazionale Dati (PDND)[62], che è stata oggetto di un nuovo investimento economico e di una rivisitazione normativa: infatti, l'art. 34 del D.L. «Semplificazioni» ha modificato l'art. 50-*ter* D.Lgs. 82/2005 (Codice dell'amministrazione digitale o CAD), che già ne dettava la disciplina di riferimento.

La PDND, introdotta dal D.Lgs. 217/2017, nasceva proprio con l'intento di superare il tradizionale «approccio "a canne d'organo", in cui, cioè, i processi tendono a svilupparsi "in

[58] D.L. 76/2020 recante «Misure urgenti per la semplificazione e l'innovazione digitale», convertito dalla L. 120/2020. Specificamente, si veda il Titolo III, dedicato alle misure di semplificazione per il sostegno e la diffusione dell'amministrazione digitale. Tra i vari interventi fatti, per esempio, il D.L. «Semplificazioni» ha modificato l'art. 3-*bis* L. 241/1990, che ora recita così: «Per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati». Tuttavia, il governo, anziché adottare una disciplina unitaria e uniforme in materia di digitalizzazione delle amministrazioni, si è, per lo più, limitato a modificare disposizioni vigenti (principalmente, del CAD), attraverso un tortuoso lavoro di sostituzione, cancellazione o integrazione degli articoli. Per un commento sugli interventi di promozione della digitalizzazione contenuti nella normativa, si veda P. CLARIZIA, *La digitalizzazione della pubblica amministrazione*, in *Giornale di diritto amministrativo*, n. 6/2020, pp. 768-781.

[59] D.L. 77/2021 recante «governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure», convertito dalla L. 108/2021. Cfr. Titolo II. Il D.L., oltre che a modificare l'art. 50 CAD sulla fruizione e riutilizzo dei dati conservati dalla PA, è ulteriormente intervenuto sull'art. 50-*ter* CAD, che si riferisce alla PDND.

[60] Il Piano Triennale è frutto della collaborazione tra AgID e Dipartimento per la trasformazione digitale (la versione aggiornata agli anni 2021-2023 del documento 2020-2022 è reperibile *online* al collegamento https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pubblica_amministrazione_2021-2023.pdf, consultato da ultimo in data 21 giugno 2022).

[61] L'Agenda 2020-2023 è stata predisposta sulla base di quanto previsto dal D.L. 76/2020, convertito con la L. 120/2020, e individua una serie di interventi prioritari, condivisi tra Governo, Regioni ed Enti Locali, definendo obiettivi, risultati attesi, responsabilità e tempi di realizzazione, anche con il coinvolgimento dei cittadini, delle imprese e delle loro associazioni; le attività previste sono realizzate in raccordo con il Piano Triennale per l'informatica nella pubblica amministrazione (documento reperibile *online* al collegamento https://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/agenda_semplificazione_2020-2023.pdf, consultato da ultimo in data 21 giugno 2022).

[62] Cfr. PNRR, op. cit., p. 93; nel documento è indicata con l'espressione "Piattaforma Nazionale Dati". Sulla PDND, si vedano P. CLARIZIA, *La digitalizzazione*, op. cit., pp. 773 e ss.; V. NERI, *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in *Urbanistica e appalti*, n. 5/2021, pp. 586-588; I. MACRÌ, Open data, open format, op. cit., pp. 1436-1438.

verticale" all'interno di unità organizzative omogenee con una scarsa propensione all'interazione con altre unità organizzative della stessa PA o peggio ancóra con altre PA»[63]. Essa «è un framework standardizzato per l'automazione della acquisizione, controllo, metadatazione e ridistribuzione sicura dei dati»[64]; detto altrimenti, consiste in un sistema in cui le diverse amministrazioni possono far canalizzare i loro dati e garantirne così una fruibilità diffusa[65]. Oltre che per motivi di efficienza, la messa in opera della Piattaforma vuole tradursi anche in una misura di semplificazione e trasparenza.

Tuttavia, anche prima di questo intervento, nell'epoca di quella che oggi definiamo Amministrazione 1.0[66], si era tentato di incentivare lo scambio di informazioni tra i vari rami della PA stabilendo che i «documenti attestanti atti, fatti, qualità e stati soggettivi, necessari per l'istruttoria del procedimento, sono acquisiti d'ufficio quando sono in possesso dell'amministrazione procedente, ovvero sono detenuti, istituzionalmente, da altre pubbliche amministrazioni» (art. 18, co. 2 L. 241/1990). Allo stesso obiettivo – all'interno del tentativo di costruire un'Amministrazione 3.0, capace di fruire delle risorse digitali offerte dalla rete Internet – mira(va) l'art. 50 CAD, che obbligava le PA a rendere i dati di loro pertinenza accessibili ad altre pubbliche amministrazioni richiedenti per lo svolgimento dei loro compiti istituzionali (co. 2) ed a rilasciare i dati in formato aperto, mettendoli a disposizione della comunità, quando non ci sono ostacoli di *privacy* o di sicurezza nazionale (co. 1).

Con la riforma del 2017 del CAD[67], avviene appunto il recepimento all'art. 50-*ter* del *Data & Analytics Framework* (DAF)[68], il prototipo della PDND. In capo alla Presidenza del Consiglio

---

[63] In questi termini, V. PATRUNO, *Il* Data & Analytics Framework *(Daf) è la Piattaforma Digitale Nazionale Dati: i punti chiave*, in www.agendadigitale.eu, 29 gennaio 2019 (reperibile *online* al collegamento https://www.agendadigitale.eu/cittadinanza-digitale/il-data-analytics-framework-daf-e-la-piattaforma-digitale-nazionale-dati-i-punti-chiave/, consultato da ultimo in data 21 giugno 2022).

[64] Così la definisce Andrea Carlini, che è stato il Responsabile per il Governo della PDND, in una breve relazione del 2019 sullo stato della Piattaforma ed i relativi piani di sviluppo, diapositiva 10 (reperibile *online* al collegamento https://cached.forges.forumpa.it/assets/Speeches/27254/co_07_carlini.pdf, consultato da ultimo in data 21 giugno 2022).

[65] Dal punto di vista tecnico, la PDND abilita l'interoperabilità dei sistemi informativi e delle basi di dati attraverso varie interfacce raccolte in un catalogo centrale API (*Application Programming Interface* o interfaccia di programmazione delle applicazioni), che permette l'accesso a dati mantenuti sempre aggiornati.

[66] Cfr. D.U. GALETTA – J.G. CORVALÁN, *Intelligenza Artificiale per una pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in www.federalismi.it, n. 3/2019, pp. 2-3 (reperibile *online* al collegamento https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=38014&dpath=document&dfile=04022019214355.pdf&content=Intelligenza%2BArtificiale%2Bper%2Buna%2BPubblica%2BAmministrazione%2B4%2E0%3F%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B, consultato da ultimo in data 21 giugno 2022). Riprendendo la classificazione fatta dai due Autori, è stato osservato come «[i]l superamento del tradizionale modello di esercizio dell'attività amministrativa, fondato sulla prevalente utilizzazione di supporti di tipo cartaceo (c.d. Amministrazione 1.0), non si risolve nel mero impiego di computer e altri apparati informatici (c.d. Amministrazione 2.0) o nella fruizione delle risorse digitali offerte dalla rete internet, dalle applicazioni mobili o dagli stessi social networks (c.d. Amministrazione 3.0), ma nell'automazione di funzioni precedentemente affidate in via esclusiva alle abilità umane (c.d. Amministrazione 4.0)». Così, V. NERI, *Diritto amministrativo*, op. cit., p. 586.

[67] La PDND è introdotta per la prima volta nel nostro ordinamento dall'art. 45 D.Lgs. 217/2017.

[68] Nel *Piano triennale per l'informatica 2017-2019* il DAF doveva far confluire i dati della PA all'interno di

dei ministri erano stati assegnati i compiti di disciplinare con apposito decreto le fasi di progettazione, sviluppo e sperimentazione di questa Piattaforma (la concreta sperimentazione, ai sensi dell'art. 50-*ter*, co. 2, era però affidata al Commissario straordinario per l'attuazione dell'Agenda digitale) finalizzata «a favorire la conoscenza e l'utilizzo del patrimonio informativo detenuto, per finalità istituzionali,» da alcune PA pilota[69], e alla «condivisione dei dati tra i soggetti che hanno diritto ad accedervi ai fini della semplificazione degli adempimenti amministrativi dei cittadini e delle imprese[70]» (art. 50-*ter*, co. 1), ma le attività di implementazione sono successivamente state sospese dalla stessa Presidenza.

Oggi, invece, invariati i fini appena detti[71], grazie all'art. 34 del D.L. «Semplificazioni» sono stati stabiliti il deciso rilancio del progetto, l'affidamento in via definitiva della gestione della predetta infrastruttura tecnologica alla Presidenza del Consiglio dei ministri (art. 50-*ter*, co. 2 CAD) e l'ampliamento dell'ambito d'applicazione della PDND anche ai gestori di servizi pubblici e a società in controllo pubblico[72]. All'AgID è stato dato il compito di adottare delle specifiche regole tecniche volte a realizzare l'armonizzazione – appunto, l'interoperabilità – dei sistemi informativi e delle basi di dati delle diverse PA che devono aderire all'infrastruttura[73].

Per quanto riguarda la trasparenza dei dati in materia di pubblici appalti per opere e servizi, sulla ripresa della messa in opera della Piattaforma la stessa Autorità nazionale anticorruzione (ANAC) non ha mancato di esprimere parere favorevole, ricordando come già nella fase di sperimentazione era già stata resa accessibile una notevole mole di informazioni presenti nella Banca Dati Nazionale dei Contratti Pubblici[74].

Tuttavia, se, da un lato, da tutti gli attori interessati è salutato positivamente il fatto che i dati detenuti dai vari rami della PA sia resi fruibili in un'ottica di semplificazione e buon andamento delle attività amministrative, dall'altro, durante la prima fase di sperimentazione sono stati sollevati dal Garante Privacy[75] dei dubbi in merito alla centralizzazione della loro gestione, che è requisito

---

un'unica piattaforma *cloud*.

[69] Cfr. artt. 2, co. 2 e 50-*ter*, co. 3 CAD.

[70] Le Camere di commercio hanno messo a disposizione delle imprese la rete camerale, che è capillare e competente sul territorio, per permettere loro il collegamento telematico con la PDND.

[71] L'art. 50-*ter*, co. 1 non è stato modificato dal D.L. «Semplificazioni». Altra finalità, che si trae da un'analisi sistematica, è quella di fare da supporto per l'armonizzazione delle procedure di servizio prioritarie indicate dal Regolamento UE n. 2018/1724 sullo Sportello unico digitale.

[72] Cfr. P. CLARIZIA, *La digitalizzazione*, op. cit., p. 773.

[73] AgID, *Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati*, ai sensi dell'articolo 50-ter, comma 2 del CAD, 2021 (reperibile *online* al collegamento https://www.agid.gov.it/sites/default/files/repository_files/lg_infrastruttura_interoperabilita_pdnd.pdf, consultato da ultimo in data 21 giugno 2022). Le Linee guida sono state adottate dall'AgID con Determinazione n. 627/2021.

[74] Cfr. ANAC, *Esame e commento*, op. cit., p. 33.

[75] Al tema del rapporto tra gli algoritmi, l'IA e il diritto alla protezione dei dati personali è prestata molta attenzione non sono in Italia, ma a livello internazionale: infatti, nel marzo del 2017 l'Information Commissioner's Office (ICO), l'autorità garante inglese, aveva pubblicato sul tema il rapporto *Big Data, artificial intelligence, machine learning and*

per far operare l'infrastruttura stessa: come è stato osservato, la creazione della PDND «comporta un accentramento e una duplicazione di tutti i dati detenuti dalle pubbliche amministrazioni per finalità del tutto generiche, realizzando di fatto una concentrazione presso un unico soggetto di informazioni, anche sensibili e sensibilissime, con evidenti rischi di vulnerabilità dei dati stessi ovvero di possibili usi distorti. La necessaria valorizzazione del patrimonio informativo pubblico non deve, infatti, avvenire a discapito della tutela dei diritti fondamentali e con possibili ricadute anche in termini di sicurezza nazionale. Un trattamento fondato sui *Big Data* in ambito pubblico richiede un'idonea base legale del trattamento che assicuri ai cittadini, oltre alla trasparenza delle decisioni, la proporzionalità del ricorso *ex lege* a tale metodologia rispetto all'obbiettivo di interesse pubblico perseguito e l'individuazione, nel rispetto del principio di *privacy by design*, di adeguate garanzie da integrare nel trattamento, dopo aver accuratamente valutato i rischi elevati per i diritti e le libertà degli interessati»[76]. Il Garante Privacy, intendendo solo evitare che si realizzino nel settore pubblico quei fenomeni di riutilizzo indeterminato ed illegittimo dei dati che più facilmente si sono riscontrati nel settore privato, è ben conscio però del fatto che non si debba «confondere l'utilizzo dell'immenso patrimonio informativo quale quello contenuto negli archivi progressivamente acquisiti e digitalizzati nel tempo dalle pubbliche amministrazioni per il perseguimento di finalità legittime e determinate, con le potenzialità insite nel fenomeno dei *Big Data*»[77].

La consapevolezza di dover disciplinare quale tipo di dati trattare e le procedure di gestione del patrimonio informativo ha portato il legislatore ad assegnare alla Presidenza del Consiglio dei ministri, gestore della Piattaforma, il compito di stabilire la «strategia nazionale dati», con la quale identificare «le tipologie, i limiti, le finalità e le modalità di messa a disposizione, su richiesta della [stessa Presidenza], dei dati aggregati e anonimizzati» di cui sono titolari i soggetti tenuti ad aderire al progetto (art. 50-*ter*, co. 4 CAD). La strategia è stabilita con decreto del Presidente del Consiglio dei Ministri, di concerto con il Ministero dell'Economia e delle Finanze e il Ministero dell'Interno, sentito il Garante Privacy e acquisito il parere della Conferenza unificata Stato-autonomie locali di

---

data protection (reperibile *online* al collegamento https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf, consultato da ultimo in data 21 giugno 2022); analogamente, la Commission National informatique et libertés (CNIL), l'Autorità garante francese, aveva pubblicato a fine 2017 il rapporto *Comment permettre à l'homme de garder la main?* (reperibile *online* al collegamento https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf, consultato da ultimo in data 21 giugno 2022).

[76] Autorità Garante della Concorrenza e del Mercato (AGCM) – Autorità per le Garanzie nelle Comunicazioni (AGCOM) – Garante per la Protezione dei Dati Personali, *Indagine conoscitiva sui* Big Data, 2020, pp. 68-69 (reperibile *online* al collegamento https://www.agcm.it/dotcmsdoc/allegati-news/IC_Big%20data_imp.pdf, consultato da ultimo in data 21 giugno 2022). Da tre prospettive diverse e complementari, l'indagine ha approfondito i cambiamenti derivanti dai *Big Data* sugli utenti che forniscono i dati, sulle aziende che li utilizzano e, dunque, sui mercati. Ciò anche al fine di cogliere appieno le possibili sinergie tra le tre Autorità e identificare gli strumenti più appropriati per eventuali interventi. Il capitolo 4 riporta le considerazioni del Garante Privacy sul possibile impatto dei *Big Data* sul diritto alla protezione dei dati personali e sulle misure e cautele da adottare.

[77] *Idem*, p. 68. A parere dello scrivente, qui il concetto di potenzialità è più che altro rivolto agli aspetti negativi determinati dal fenomeno dei *Big Data*.

cui all'art. 8 D.Lgs. 281/1997.

Ad ogni modo, per espressa previsione, nella PDND «non confluiscono i dati attinenti a ordine e sicurezza pubblici, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria» (art. 50-*ter*, co. 3 CAD). Quest'ultima disposizione è importante perché permette di fare alcune considerazioni sulle banche dati che potranno essere utilizzate per far funzionare i dispositivi di polizia predittiva (v. *infra*): infatti, le autorità e le forze di polizia che si occupano di prevenzione e repressione del reato non potranno fare affidamento sulla Piattaforma per trarre dati con cui alimentare questa specifica strumentazione di cui si è accennato e che sarà analizzata oltre, ma dovranno eventualmente implementare un'infrastruttura *ad hoc*. Per quanto può interessare circa questo specifico punto, anticipiamo che l'ambito di applicazione di queste macchine è confinato a limitate aree territoriali, di modo che l'elaborazione algoritmica possa prevedere – e così prevenire – la reiterazione di specifici fenomeni criminali che avvengono con particolari modalità in aree precise. Nell'evenienza in cui tutte le Questure fossero dotate di dispositivi di polizia predittiva, ne conseguirebbe che ognuna dovrebbe curare da sé l'inserimento dei dati tratti dai fenomeni criminali avvenuti nel territorio di competenza nella propria banca dati. Fermi protocolli unici nazionali di funzionamento dei dispositivi e di trattazione dei dati da parte degli agenti di polizia, pensare ad un'unica piattaforma potrebbe essere controproducente, dal punto di vista della risposta locale delle forze di polizia, in quanto l'accuratezza delle previsioni ne risulterebbe azzoppata da un contesto spaziale di riferimento eccessivamente grande. La creazione di una connessione tra tutte queste banche dati locali, invece, potrebbe essere utile per favorire la scoperta di gruppi criminali operanti a livello nazionale e permettere indagini tradizionali sul loro conto: infatti, gli algoritmi di IA potrebbero collegare a disegni criminali di ampia portata eventi di reato con particolari caratteristiche che, altrimenti, finirebbero per essere ritenuti limitati al contesto locale.

In generale, trovandoci tuttora nel pieno delle fasi e coinvolgimento degli enti detentori delle principali banche dati di interesse nazionale e condivisione delle informazioni per rendere operativa la PDND, non è ancóra possibile capire se nei fatti si saranno realizzati gli effettivi miglioramenti auspicati dal Governo, ma la circostanza stessa della decisa ripresa in considerazione del progetto di cambiamento dell'architettura amministrativa e delle modalità di interconnessione tra le basi dati delle PA è sicuramente da considerarsi cosa positiva.

Parallelamente alla Piattaforma Digitale Nazionale Dati, anche per lo specifico settore dei contratti pubblici è in fase di realizzazione la digitalizzazione delle procedure per l'assegnazione di opere e servizi (*e-procurement*) stabilita dall'art. 44 del Codice dei contratti pubblici (D.Lgs. 50/2016). Il decreto interministeriale, che definisce «le modalità di digitalizzazione delle procedure di tutti i contratti pubblici, anche attraverso l'interconnessione per interoperabilità dei dati delle

pubbliche amministrazioni», nonché «le migliori pratiche riguardanti metodologie organizzative e di lavoro, metodologie di programmazione e pianificazione, riferite anche all'individuazione dei dati rilevanti, alla loro raccolta, gestione ed elaborazione, soluzioni informatiche, telematiche e tecnologiche di supporto», avrebbe dovuto vedere la luce entro un anno dall'entrata in vigore del Codice dei contratti pubblici. Solo recentemente, però, con la pubblicazione del D.M. 148/2021, si è adempiuto in tal senso, spinti, oltre che dalle indicazioni contenute nelle Direttive europee in materia di appalti e concessioni[78], anche dalla necessità di garantire semplificazione, trasparenza, efficienza e tempestività alle procedure afferenti i contratti pubblici, particolarmente importanti nella congiuntura economica presente, con le risorse del PNRR in attesa di essere spese in modo veloce ed efficace.

Tuttavia, più che un decreto attuativo, il regolamento delinea i principi generali cui dovranno attenersi le Linee guida AgID, che renderanno effettivamente operativa la digitalizzazione (art. 2 D.M. 148/2021). I suoi contenuti restano, infatti, mere petizioni di principio, tanto che l'obbligo di adeguare i sistemi telematici delle stazioni appaltanti scatta soltanto sei mesi dopo l'adozione delle citate Linee guida, per l'elaborazione delle quali il decreto non assegna alcun termine (art. 29 D.M. 148/2021). Concretamente, l'adozione di tale sistema renderà semplice e spedito l'*iter* di gara: aiuterà stazioni appaltanti e operatori economici a redigere i documenti e gli atti di propria competenza, consentirà il tracciamento di tutte le operazioni svolte e supporterà ogni fase della procedura di gara, potendo contare sull'interoperabilità sia con i sistemi contabili delle stazioni appaltanti sia con i sistemi rilevanti ai fini della semplificazione delle procedure per gli operatori economici.

Nel generale utilizzo, per quanto agli albori, di algoritmi più o meno evoluti nelle fasi procedimentali che incidono sulle forme di manifestazione della potestà pubblica (Amministrazione 4.0) e che hanno già portato il Consiglio di Stato ad esprimersi in merito con la citata sentenza n. 2270/2019, di fronte all'intenzione dell'esecutivo di utilizzare tale tecnologia nelle fasi procedimentali finalizzate all'assegnazione degli appalti, lo stesso Consiglio di Stato, interpellato in merito, aveva emesso un parere sullo schema di decreto ministeriale recante le modalità di digitalizzazione delle procedure dei contratti pubblici[79]. In tale occasione, è stato sottolineato come «la commissione giudicatrice deve rimanere […] il solo organo deputato alla valutazione delle offerte tecniche ed economiche ed all'assegnazione dei relativi punteggi, potendosi demandare al sistema telematico unicamente lo svolgimento di compiti prettamente aritmetici […,] purché

[78] Ci si riferisce alla Direttiva UE n. 2014/24, avente ad oggetto gli appalti per i settori ordinari, alla Direttiva UE n. 2014/25, avente ad oggetto gli appalti per i c.d. settori speciali, e alla Direttiva UE n. 2014/23 in materia di concessioni, che avevano portato alla riforma del Codice dei contratti pubblici nel 2016.

[79] Consiglio di Stato, Sezione consultiva per gli atti normativi, parere n. 1940 del 26.11.2020 sullo schema di decreto ministeriale recante le modalità di digitalizzazione delle procedure dei contratti pubblici.

rimanga sempre escluso che il sistema telematico possa sostituirsi alla commissione giudicatrice nell'esercizio del suo potere tecnico-discrezionale». In definitiva, è necessario «garantire espressamente che l'utilizzo del sistema telematico non comprometta o pregiudichi la normativa primaria di svolgimento della procedura di evidenza pubblica, non si appropri di spazi di discrezionalità tecnica riconosciuti agli organi della stazione appaltante, assicuri il rispetto delle regole di riservatezza delle sedute non pubbliche della commissione giudicatrice e l'osservanza di quelle relative all'accesso agli atti di gara».

Questo significa che, anche nel settore dei pubblici appalti, se, da una parte, l'uso di algoritmi di IA in ottica di maggior efficienza e generale buon andamento dell'azione amministrativa (art. 97 Cost.) non è ostacolato, ma anzi auspicabile, dall'altra non si è mancato di ribadire il ruolo ancillare che questi devono mantenere nei confronti del Responsabile del procedimento. Nella generale attività amministrativa, non si tratta di «sostituire con un algoritmo la figura del funzionario responsabile del procedimento: piuttosto, è viceversa certamente possibile immaginare che il funzionario responsabile si serva utilmente dell'Intelligenza Artificiale»[80].

Ad ogni modo, anche se importanti principi attuativi e linee guida sull'automazione della funzione amministrativa si ricavano nella sentenza 2270/2019 del Consiglio di Stato, che ha delineato uno statuto dell'algoritmo nel procedimento, e dal *Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino*[81] pubblicato dall'AgID, con il quale è stata esaminata l'incidenza delle più avanzate tecnologie informatiche sulle forme di svolgimento delle relazioni sociali e sul tradizionale modello di esercizio dell'attività amministrativa, «il quadro delle norme vigenti sull'utilizzo dei *software* di intelligenza artificiale nel settore giuspubblicistico appare scarno e lacunoso»[82]. L'art. 3-*bis* L. 241/1990, nella formulazione risultante dalle modifiche introdotte dal D.L. «Semplificazioni», si limita, infatti, a disporre che, «[p]er conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati». Allo stesso modo, l'art. 50-*ter* CAD, nel prescrivere l'istituzione della PDND, «disciplina l'utilizzo delle tecnologie informatiche esclusivamente sotto il profilo della interconnessione dei sistemi informativi delle PA»[83], nulla dicendo sull'eventuale impiego di algoritmi in ambito amministrativo; lo stesso dicasi per la digitalizzazione delle procedure di cui all'art. 44 Codice dei contratti pubblici.

Dunque, come già si ha avuto modo di constatare per l'ambito della gestione della giustizia (v. *supra*), l'Italia è ancóra impegnata a completare il processo di digitalizzazione della struttura

[80] Così, D.U. GALETTA – J.G. CORVALÁN, *Intelligenza Artificiale per una pubblica Amministrazione 4.0?*, op. cit., p. 17.
[81] Task Force IA dell'AgID, *Libro Bianco sull'Intelligenza Artificiale*, op. cit.
[82] In questi termini, V. NERI, *Diritto amministrativo*, op. cit., p. 587.
[83] *Idem*, p. 587.

amministrativa, che è prerequisito per il funzionamento dell'intelligenza artificiale. Nonostante i tentativi in avanti di cui si è detto ed i propositi raccolti in testi ricognitivi, ad oggi mancano totalmente una decisa programmazione e sperimentazione dell'IA in campo amministrativo per lo svolgimento delle attività ordinarie e, a maggior ragione, per finalità in senso stretto di anticorruzione.

Eppure, recentemente è stato introdotto nel nostro ordinamento uno strumento che, puntando espressamente sulla digitalizzazione, pare avere *in nuce* anche l'utilizzo di algoritmi per la prevenzione del rischio corruzione e aprire le porte alla loro sperimentazione. Con l'art. 6 D.L. 80/2021[84] è stato istituito il Piano Integrato di Attività e Organizzazione (PIAO)[85], perseguendo la finalità di «assicurare la qualità e la trasparenza dell'attività amministrativa e migliorare la qualità dei servizi ai cittadini e alle imprese e procedere alla costante e progressiva semplificazione e reingegnerizzazione dei processi anche in materia di diritto di accesso» (co. 1). Il PIAO deve essere adottato, entro il 31 gennaio di ogni anno, dalle pubbliche amministrazioni con più di cinquanta dipendenti, con esclusione delle scuole di ogni ordine e grado e delle istituzioni educative, e si compone di quattro sezioni: 1) scheda anagrafica dell'Amministrazione; 2) valore pubblico, *performance* e anticorruzione; 3) organizzazione e capitale umano; 4) monitoraggio[86]. Il Piano, di durata triennale e aggiornato annualmente, ha l'obiettivo di assorbire, in un'ottica di razionalizzazione e semplificazione, molti degli atti di pianificazione cui sono tenute le Amministrazioni[87]; a tal fine, un apposito D.P.R. avrà il compito di identificare gli adempimenti oggetto di abrogazione[88].

---

[84] Decreto «Reclutamento PA», convertito con L. 113/2021.

[85] In merito, si vedano A.M. SAVAZZI – R. CARDAMONE, *Il Piano Integrato di Attività e Organizzazione (PIAO)*, in *Azienditalia*, n. 4/2022, pp. 775-784; B. SUSIO – E. BARBAGALLO, *Dal PTPCT al PIAO: la strategia di prevenzione della corruzione fa sinergia e si rafforza*, in *Azienditalia*, n. 4/2022, pp. 699-706.

[86] Cfr. Presidenza del Consiglio dei ministri – Dipartimento della Funzione Pubblica, *Linee Guida per la compilazione del Piano Integrato di Attività e Organizzazione (PIAO)*, circolare 6 dicembre 2021 (reperibile *online* al collegamento https://www.astrid-online.it/static/upload/pian/piano-piao---linee--guida-6-dicembre-2021.pdf, consultato da ultimo in data 21 giugno 2022).

[87] Il PIAO sostituisce i seguenti strumenti di pianificazione: il Piano degli obiettivi (PDO**)**, poiché dovrà definire gli obiettivi programmatici e strategici della prestazione, stabilendo il collegamento tra l'attività individuale e i risultati della prestazione globale dell'ente; il Piano Organizzativo del Lavoro Agile (POLA) e il Piano della Formazione, poiché definisce la strategia di gestione del capitale umano e dello sviluppo organizzativo; il Piano triennale del fabbisogno del personale, poiché dovrà definire gli strumenti e gli obiettivi del reclutamento di nuove risorse e la valorizzazione delle risorse interne; il Piano anticorruzione (PTPCT), così da raggiungere la piena trasparenza nelle attività di organizzazione. A ben vedere, l'assetto normativo attuale già forniva gli strumenti e i presidi nella direzione dell'integrazione tra il ciclo della prestazione, la pianificazione dei fabbisogni di personale e il piano di prevenzione della corruzione (artt. 6 D.Lgs. 165/2001 e 44 D.Lgs. 33/2013). Tuttavia, il nuovo PIAO impone alle Amministrazioni di pervenire ad una visione unitaria di processi di programmazione, che fino ad oggi si sviluppavano in completa autonomia, spesso governati da strutture diverse della stessa Amministrazione.

[88] Il Consiglio di Stato, Sezione consultiva per gli atti normativi, con parere n. 506 del 02.03.2022, si è espresso sullo schema di D.P.R. recante l'individuazione e abrogazione degli adempimenti relativi ai piani assorbiti dal PIAO, consigliando molte modifiche e una più incisiva razionalizzazione del sistema pianificazione, che porti non solo ad abrogare «le norme incompatibili», ma a conservare solo le norme, tra quelle rimaste in vigore, «davvero indispensabili» (par. 3.4).

Tra gli altri obiettivi indicati all'art. 6, co. 2, il PIAO definisce anche «gli *strumenti* e le fasi per giungere alla piena trasparenza dei risultati, dell'attività e dell'organizzazione amministrativa nonché per raggiungere gli obiettivi in materia di contrasto alla corruzione, secondo quanto previsto dalla normativa vigente in materia e in conformità agli indirizzi adottati dall'Autorità nazionale anticorruzione con il Piano nazionale anticorruzione» (co. 2, lett. d))[89].

Prima di procedere con l'analisi che qui interessa, merita precisare *en passant* come il PIAO, nella strategia di integrazione e semplificazione degli strumenti di programmazione, finisca per inglobare le tematiche proprie del Piano triennale di prevenzione della corruzione e della trasparenza (PTPCT), di fatto sostituendolo; come precisato nel D.M. del Ministro per la Funzione Pubblica del 1 dicembre 2021, che introduce il Piano-tipo, e nelle *Linee guida per la compilazione del PIAO*, la sottosezione del Piano denominata "*Rischi corruttivi e trasparenza*", predisposta dal Responsabile della prevenzione della corruzione e della trasparenza, contiene quanto già previsto per il PTPCT[90].

Tornando alla norma, il riferimento specifico agli «strumenti […] per raggiungere gli obiettivi in materia di contrasto alla corruzione» è, a parere di chi scrive, un passo in avanti nel fornire un formale appiglio normativo alle pubbliche amministrazioni, che, nel predisporre il proprio PIAO tarandolo sulle proprie esigenze, vorranno eventualmente sperimentare l'utilizzo dell'intelligenza artificiale in attività di monitoraggio e gestione del rischio corruzione. Al contrario, nel recente passato la normativa e gli atti di indirizzo in materia di anticorruzione erano abbastanza vaghi o facevano riferimento all'adozione di misure organizzative tradizionali per la prevenzione della corruzione: infatti, l'art. 1, co 5 L. 190/2012, nell'introdurre l'istituto del PTPCT, stabiliva genericamente che questo dovesse indicare «interventi organizzativi» volti a prevenire il rischio di corruzione; parimenti, l'ultimo *Piano nazionale anticorruzione* (PNA)[91], adottato dall'ANAC,

[89] Corsivo mio. Il modo in cui era stato formulato l'art. 6 D.L. 80/2021 aveva fatto sorgere qualche dubbio su quale fosse l'Autorità competente in materia di anticorruzione in relazione agli interventi previsti nel PNRR (se gli uffici governativi o, appunto, l'ANAC). Infatti, è lecito attendersi che il Piano di prevenzione della corruzione possa essere ricompreso tra quelli che saranno abrogati ed assorbiti nel nuovo PIAO, consistendo il suo contenuto anche nell'individuazione di misure (strumenti) per il trattamento del rischio residuo di corruzione e nella loro programmazione (fasi) anche in termini di tempi di attuazione e di relative responsabilità. Di qui la preoccupazione espressa dall'attuale Presidente Giuseppe Busia in merito al rischio di un significativo indebolimento delle funzioni di regolazione, vigilanza, ordine e sanzionatorie dell'ANAC e la conseguente richiesta di emendamenti correttivi. Tra i vari emendamenti proposti dal presidente dell'ANAC – e poi accolti in sede di conversione del D.L. – vi era appunto quello all'articolo 6, co. 2, lett. d), volto a far sì che il PIAO si dovesse conformare alle indicazioni dell'ANAC contenute nel Piano nazionale anticorruzione. Il recepimento della modifica sembrerebbe quindi aver ristabilito la centralità dell'Autorità nazionale anticorruzione nelle politiche pubbliche in materia di prevenzione e contrasto alla corruzione. Sul punto e sul ruolo dell'ANAC, si veda C. BENETAZZO, *Gli appalti pubblici nel PNRR*, op. cit., pp. 130 e ss.

[90] Cfr. B. SUSIO – E. BARBAGALLO, *Dal PTPCT al PIAO*, op. cit., p. 702.

[91] L'ultimo PNA di riferimento è quello del 2019 (tutti i Piani nazionali anticorruzione adottati dall'ANAC dal 2013 in poi sono reperibili *online* al collegamento https://www.anticorruzione.it/portal/public/classic/Attivitadocumentazione/Anticorruzione/PianoNazionaleAnticorruzione, consultato da ultimo in data 21 giugno 2022).

sottolineava come spetti alle singole amministrazioni «valutare e gestire il rischio corruttivo, secondo una metodologia che comprende l'analisi del contesto (interno ed esterno), la valutazione del rischio (identificazione, analisi e ponderazione del rischio) e il trattamento del rischio (*identificazione e programmazione delle misure di prevenzione*)»[92]. Diversamente, le *Linee guida per la compilazione del PIAO*, adottate nel nuovo contesto di forte spinta alla digitalizzazione della PA e all'adozione di nuove tecnologie per efficientarne il funzionamento, stabiliscono esplicitamente che, in fase di individuazione degli accorgimenti organizzativi per il trattamento del rischio corruzione, devono «essere privilegiate le misure volte a raggiungere più finalità, prime fra tutte quelli di semplificazione, efficacia, efficienza ed economicità [, rivolgendo particolare favore] alla predisposizione di *misure di digitalizzazione*»[93].

In definitiva, con la forte spinta alla digitalizzazione di tutto l'apparato amministrativo e di procedure tradizionalmente interessate dal fenomeno corruttivo quali quelle relative ai bandi di gara[94], la possibilità di adottare sistemi in grado di monitorare e gestire il rischio corruzione, prevedendone quindi l'applicazione nel PTPCT (per le amministrazioni non destinatarie della disposizione di cui all'art. 6 D.L. 80/2021) e nel PIAO, si concretizza sempre di più, per quanto sia ancóra di là da venire.

L'IA, potendo processare enormi quantità di dati, si può rivelare uno strumento formidabile per l'identificazione di profili di anomalia (*red flags*) e di situazioni a potenziale rischio-corruzione (v. *infra*). «La prospettiva, che oggi inizia a manifestarsi concretamente, è quella della *automazione* della *compliance*[95] anticorruzione, tanto nel settore pubblico quanto in quello privato, come potenziale rivoluzione del modo di intendere le attività di prevenzione dei reati, passandosi da un sistema basato per lo più sul lavoro in *team* e su controlli a campione "sul campo" a una metodologia innovativa volta a sfruttare la straordinaria capacità computazionale dei *software*

---

[92] ANAC, *Piano nazionale anticorruzione 2019*, adottato con delibera n. 1064/2019, Parte II, par. 1, p. 17 (reperibile *online* al collegamento https://www.anticorruzione.it/documents/91439/4c582909-32e4-2112-8c98-046a72082d4a, consultato da ultimo in data 21 giugno 2022); corsivo mio. Sempre di «misure» si parla nelle indicazioni metodologiche contenute nell'Allegato 1, pp. 40 e ss., a cui rinvia lo stesso PNA (reperibile *online* al collegamento https://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/Allegato%201%20-%20PNA%202019S.pdf, consultato da ultimo in data 21 giugno 2022).

[93] Cfr. Presidenza del Consiglio dei ministri – Dipartimento della Funzione Pubblica, *Linee Guida per la compilazione del Piano Integrato*, op. cit., Sez. 2, Sottosez. di programmazione: *Rischi corruttivi e trasparenza*; corsivo mio.

[94] Cfr. ANAC, *La corruzione in Italia (2016-2019). Numeri, luoghi e contropartite del malaffare*, 2019, p. 2 (reperibile *online* al collegamento https://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/Anticorruzione/MisurazioneTerritorialeRischio/RELAZIONE%20+%20TABELLE-rev3.pdf, consultato da ultimo in data 21 giugno 2022). Dal rapporto emerge che oltre il 74% delle vicende corruttive registratesi in Italia fra agosto 2016 e agosto 2019 (pari a 113 casi) ha riguardato l'assegnazione di appalti pubblici, a conferma dell'ingente volume economico e degli interessi illeciti legati al settore.

[95] La "*compliance*" può intendersi come il controllo dell'esatta applicazione della norma, della conformità dell'operato ai dettami di legge.

informatici di mettere in correlazione comportamenti, identificando *pattern*, segnali di allarme e altri fattori di rischio non individuabili altrimenti»[96].

Tuttavia, poco si è riflettuto sulle implicazioni che lo sviluppo di tali procedure potrà avere nelle attività di controllo di conformità: infatti, si potrà passare «da un sistema che ruota attorno alle classiche attività umane di analisi e indagini preventive "sul campo", a un sistema (parzialmente o integralmente) automatizzato in cui è la sola "macchina" ad assumere su di sé il ruolo di valutare il rischio e di individuare le procedure per gestirlo – e in cui l'uomo svolge soltanto il compito di assicurarsi che il *software* intelligente abbia riserve di "carburante" (cioè dati) sufficienti a poter svolgere i propri adempimenti di sorveglianza»[97].

A tal proposito, si pensi alla possibilità di utilizzare per il contrasto alla corruzione la tecnologia *blockchain* all'interno dei processi decisionali delle organizzazioni complesse pubbliche o private (ove le figure operative e gli organi di controllo potrebbero costituire i vari nodi della catena di blocchi) col fine di assicurare trasparenza, efficienza e immodificabilità dei dati raccolti[98]: ciò consentirebbe di «agire su tempi e costi di esecuzione delle attività (anche attraverso la razionalizzazione dei controlli), svincolare le dinamiche gestionali da distorsioni legate a rapporti personali e conflitti d'interesse, assicurare scelte consapevoli e condivise e, non secondari, impatti sul contenzioso»[99].

Più avanti saranno analizzati i vantaggi e i rischi derivanti dall'adozione di strumenti informatici di *big data analytics*, evidenziando come tali prassi possano diventare strumento di prevenzione del rischio di corruzione nei settori pubblico e privato, a patto che il legislatore regolamenti il fenomeno per trovare un bilanciamento tra le legittime misure anticorruzione e i diritti della persona sottoposta a controllo. Se nel settore pubblico si tratta di stabilire delle regole *ad hoc* in materia di anticorruzione sulla scia di orientamenti giurisprudenziali e pronunce delle Autorità indipendenti in merito al rapporto tra IA e diritto, nel settore privato si dovrà giungere ad una riforma coerente del D.Lgs. 231/2001 sulla responsabilità amministrativa delle persone giuridiche, in quanto la necessità per gli enti collettivi di adottare cautele interne per evitare che i

---

[96] In questi termini, P. SEVERINO, *Corruzione e crisi pandemica*, op. cit., p. 1891.

[97] Così, E. BIRRITTERI, Big Data Analytics *e* compliance *anticorruzione*, op. cit., p. 291.

[98] In generale, per un'analisi delle connessioni tra corruzione, *blockchain* e *bitcoin*, si veda N. KOSSOW – V. DYKES, *Blockchain, bitcoin and corruption. A review of the linkages*, in *Transparency International Anti-Corruption Helpdesk Answer*, 22 gennaio 2018 (reperibile online al collegamento https://knowledgehub.transparency.org/assets/uploads/helpdesk/Blockchain-bitcoin-and-corruption-2018.pdf, consultato da ultimo in data 21 giugno 2022). Invece, sul tema dell'uso della *blockchain* nella pubblica amministrazione, si veda M. MACCHIA, *Blockchain e pubblica amministrazione*, in www.federalismi.it, n. 2/2021, pp. 117-129 (reperibile *online* al collegamento https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=44796&dpath=document&dfile=18012021001855.pdf&content=Blockchain%2Be%2Bpubblica%2Bamministrazione%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B, consultato da ultimo in data 21 giugno 2022).

[99] Così, G. CARIOLA, *Così la blockchain aggiorna i controlli interni*, in www.ntplusfisco.ilsole24ore.com (*Quotidiano del Fisco* – il Sole24ore), 16 febbraio 2019.

propri dipendenti commettano dei reati nello svolgimento dell'attività lavorativa si scontra con lacune giuridiche e principi sistematici che ne impediscono o rendono incerta l'adozione.

2.2 Gli strumenti di polizia predittiva[100].

All'interno del contesto della società della sorveglianza e nel generale fenomeno di confluenza a fini preventivi del diritto penale nel diritto amministrativo spicca, come detto, anche l'impiego da parte delle forze di polizia di dispositivi informatici di polizia predittiva[101] che, ipotizzando dove e quando si verificherà la commissione dei reati, permettono di prevenirne efficacemente[102] la commissione con adeguata azione di pattugliamento (*patrolling*) e, quindi, di meglio assolvere al compito assegnatogli di vigilare sulla pubblica sicurezza[103]; in questo modo, si ottiene il duplice risultato di garantire più sicurezza ai cittadini e sfruttare al meglio le risorse e le energie disponibili. Dunque, la qualità di un qualsiasi programma di polizia predittiva «si misura sul numero di episodi di reato che riesce a prevenire: una valutazione di efficacia facilmente oggettivabile, e come tale valutabile in termini trasparenti»[104].

Fino a qualche anno fa, il «termine evocativo, dal sapore scientifico»[105], "Precrimine" avrebbe semplicemente fatto pensare al racconto di finzione *Minority Report* di Philiph K. Dick[106],

---

[100] «Secondo me, […] avremo indubbiamente un altro [crimine]. Molto dipende dalla *chance*. Finora il nostro *inconnu* è stato fortunato. Ma, d'ora in poi, può darsi che la fortuna gli volti le spalle. In ogni modo, dopo un altro delitto, ne sapremo molto, ma molto di più. Perché, vedete, il delitto è enormemente rivelatore! Per quanto i metodi possano variare, gusti, abitudini, comportamenti emergono puntualmente nelle nostre azioni. […] presto i contorni diventeranno più netti e, finalmente, "io saprò…" […] Non conoscerò né il suo nome, né l'indirizzo! Ma saprò *che tipo di uomo è*…» (Hercule Poirot). A. CHRISTIE, *La serie infernale*, Mondadori, Milano 2012, 35 ed., p. 110. «La prevenzione di ciò che non è accaduto attira l'evento» (Javier Marías).

[101] Cfr. M. MENDOLA, *One Step Further in the "Surveillance Society": The Case of Predictive Policing*, Tech and Law Center, 17 ottobre 2016, p. 2 (reperibile *online* al collegamento https://www.slideshare.net/TechAndLaw/one-step-further-in-the-surveillance-society-the-case-of-predictive-policing-67277049, consultato da ultimo in data 21 giugno 2022), quando afferma che la «*"Predictive Policing" shall be considered one of the last technological applications within the context of surveillance society*» (tradotto: la «"Polizia Predittiva" può essere considerata una delle ultime applicazioni tecnologiche all'interno del contesto della società della sorveglianza»).

[102] I dubbi manifestati da alcuni non riguardano tanto l'efficacia di tali dispositivi, quanto i rischi che il loro utilizzo comporterebbe. Sul punto, si veda *infra*.

[103] Per un completo inquadramento della materia della Polizia Predittiva, anche se con riferimento al solo contesto statunitense, si vedano 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 (reperibile *online* al collegamento https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf, consultato da ultimo in data 21 giugno 2022); A.G. FERGUSON, *Policing Predictive Policing*, in *Washington University Law Review*, vol. 94, n. 5/2017, pp. 1109-1189 (reperibile *online* al collegamento https://openscholarship.wustl.edu/law_lawreview/vol94/iss5/5/, consultato da ultimo in data 21 giugno 2022).

[104] Cosi, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 56.

[105] In questi termini, R. PELLICCIA, *Polizia Predittiva: il futuro della prevenzione criminale?*, in www.cyberlaws.it, 9 maggio 2019, p. 1 (reperibile *online* al collegamento https://www.cyberlaws.it/2019/polizia-predittiva-il-futuro-della-prevenzione-criminale/, consultato da ultimo in data 21 giugno 2022).

[106] P.K. DICK, *The Minority Report*, in *Fantastic Universe*, vol. 4, 1956, pp. 4-36; trad. it. *Rapporto di minoranza*, in *Rapporto di minoranza e altri racconti*, Fanucci, Roma 2002.

che narra di un sistema di controllo – il Precrimine (*Precrime*), appunto – basato sulle premonizioni di tre individui, i *Precog*, tenuti in stato di semicoscienza e capaci di individuare in modo infallibile i futuri omicidi. Il sistema sembra funzionare perfettamente perché, dopo cinque anni di sperimentazione, «*has cut down felonies by ninety-nine and decimal point eight percent*»[107] e nessun omicidio è più stato commesso a Washington, D.C., realizzando così nel 2054 il sogno di una città senza crimine. Resta, tuttavia, il problema dello statuto di colpevolezza degli individui – dei «*would-be criminals*»[108] – inviati al contenimento, in quanto il loro arresto è avvenuto prima del reato ed essi sono quindi tecnicamente innocenti, ma questo per le autorità costituite – secondo una logica di prevenzione, del controllo capillare sui cittadini – sembra un prezzo da pagare accettabile nella lotta al crimine[109].

Oggi, invece, tralasciando «sistemi che azzardano sulla possibilità di catturare l'autore [di un crimine] nel momento in cui [lo] commette […] come nel caso del [Precrimine]»[110] ed i cui fini tendono direttamente ad individuare a priori il criminale e neutralizzarlo[111], l'idea di anticipare le mosse della criminalità si è concretizzata, grazie alla tecnologia ed agli algoritmi, in sistemi di polizia predittiva che supportano le forze di polizia nell'espletare il loro compito di polizia di prevenzione attraverso la segnalazione di serie criminali realizzate dagli stessi soggetti e l'analisi e la gestione del territorio in funzione della sua vulnerabilità.

Ora, per "polizia predittiva" (*Predictive Policing*) si intende «l'insieme delle attività rivolte allo studio e all'applicazione di metodi statistici con l'obiettivo di "predire" *chi* potrà commettere un reato, o *dove* e *quando* potrà essere commesso un reato, al fine di prevenire la commissione dei reati stessi»[112]. Nell'ottica di superare l'impostazione che voleva l'attività di polizia concepita in

---

[107] Tradotto: «ha permesso di ridurre i crimini del 99.8 per cento». P.K. DICK, *Rapporto di minoranza*, op. cit, p. 31.

[108] Tradotto: «potenziali criminali». *Idem*, op. cit, p. 29.

[109] Per un'analisi filosofico-giuridica del testo di Philiph K. Dick, che esula dalla presente trattazione, si veda T. GAZZOLO, Minority Report *e il crimine senza crimine*, in www.jus.vitaepensiero.it, vol. 6, n. 1/2020, pp. 224-251 (reperibile *online* al collegamento principale https://jusvitaepensiero.mediabiblos.it/archivio/Vol.%20VI,%20N.%201,%20Febbraio%202020.pdf, oppure al collegamento secondario https://jus.vitaepensiero.it/news-papers-minority-report-e-il-crimine-senza-crimine-5281.html, consultati da ultimo in data 21 giugno 2022).

[110] In questi termini, E. LOMBARDO, *Intelligenza Artificiale e* human intelligence *per la prevenzione dei crimini*, Società italiana di Intelligence Press, 2020, p. 15 (reperibile *online* al collegamento https://press.socint.org/index.php/home/catalog/view/2020_07_lombardo/17/36-1, consultato da ultimo in data 21 giugno 2022).

[111] Cfr. D. BENEDETTI, *IA e (in)sicurezza informatica*, op. cit., pp. 253-254.

[112] Così, F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 10. Analogamente, W.L. PERRY – B. MCINNIS – C.C. PRICE – S.C. SMITH – J.S. HOLLYWOOD, *Predictive Policing*, op. cit., pp. 1-2, affermano che «*[p]redictive 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*» (tradotto: «La polizia predittiva è l'applicazione di tecniche analitiche – specialmente tecniche quantitative – per identificare probabili obiettivi per l'intervento della polizia e prevenire il crimine o risolvere crimini del passato attraverso l'elaborazione di predizioni statistiche»); B. PEARSALL, *Predictive Policing: The Future of Law Enforcement?*, in *NIJ Journal,* n. 266, 2010 (reperibile *online* al collegamento https://nij.ojp.gov/topics/articles/predictive-policing-future-law-enforcement, consultato da ultimo in data 21 giugno 2022), la definisce essenzialmente come «*taking data from disparate sources, analyzing them and then using the results to anticipate, prevent and respond more effectively to future crime*» (tradotto:

termini tradizionalmente reattivi, cioè di mera repressione dei crimini già avvenuti, si è dapprima iniziato a raccogliere ed esaminare informazioni e dati per creare dei modelli comportamentali dei criminali a favore di un'attività anche preventiva; successivamente, «[m]uovendo dall'assunto che per prevenire bisogna prevedere»[113], grazie alla grande disponibilità di dati ed alla diffusione di algoritmi capaci di raccoglierli e rielaborarli per estrarne informazioni e scoprire «connessioni prima difficilmente individuabili dall'operatore umano»[114] (*data mining*)[115], si è mirato ad analizzare e visualizzare in ottica futura le tendenze ed i modelli criminali costruiti per prevenire la realizzazione di specifici crimini oggetto della statistica, andando così a delineare un risposta proattiva[116].

Mentre le tecniche di prevenzione adottate in passato[117] dalle forze di polizia, pur focalizzandosi sull'analisi delle informazioni, piuttosto che sullo studio delle cause scatenanti il crimine, si limitavano a fotografare il presente, la polizia predittiva si caratterizza per «*the explicit projection into the future*»[118], in quanto fornisce continue previsioni aggiornate sulla base dei nuovi dati raccolti. Comunque, punto comune tra tutti i vecchi approcci ed i nuovi sistemi di polizia predittiva è il crescente ruolo riconosciuto alle attività di *intelligence* – intese come ricerca e raccolta di informazioni – affianco alle tradizionali operazioni di polizia, tanto che la polizia predittiva può essere ritenuta diretta evoluzione dell'approccio basato sulla valutazione e gestione del rischio (*intelligence-led policing*)[119].

«prendere dati da fonti disparate, analizzarli e poi usarne i risultati per anticipare, prevenire e rispondere più efficacemente ai futuri crimini»). La National Institute of Justice (NIJ), nella cui rivista è stata data quest'ultima definizione, è l'agenzia di ricerca, sviluppo e valutazione del Dipartimento di Giustizia degli Stati Uniti.

[113] In questi termini, S. SIGNORATO, *Giustizia penale e intelligenza artificiale*, op. cit., p. 607.

[114] Così, F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 10. Cfr. C. CATH – S. WACHTER – B. MITTELSTADT – M. TADDEO – L. FLORIDI, *Artificial Intelligence and the "Good Society"*, op. cit., e L. BENNETT MOSES – J. CHAN, *Algorithmic prediction in policing: assumptions, evaluation, and accountability*, in *Policing and Society*, vol. 28, n. 7/2018, pp. 806 e ss. (reperibile *online* al collegamento https://www.tandfonline.com/doi/full/10.1080/10439463.2016.1253695, consultato da ultimo in data 21 giugno 2022). Proprio il fatto di esprimere la massima utilità ed efficacia nella ricerca di specifici legami o modelli (*pattern*) all'interno di banche dati con grandissime mole di dati rende le applicazioni di intelligenza artificiale importanti nell'ambito della pubblica sicurezza.

[115] Cfr. R. PELLICCIA, *Polizia Predittiva*, op. cit. p. 2, secondo cui «[g]li algoritmi di data mining si sono rivelati […] il vero fulcro del progetto di polizia predittiva».

[116] Per una breve panoramica sulle indagini preventive, repressive e proattive (rispettivamente *pretrial investigations*, *reactive investigations* e *proactive investigations*), seppur lì viste nello specifico ambito delle indagini informatiche (*cyber investigations*), si veda S. SIGNORATO, *Tipologie e caratteristiche delle* cyber investigations *in un mondo globalizzato*, in *Diritto Penale Contemporaneo*, fasc. n. 3/2016, pp. 194-195 (reperibile *online* al collegamento https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_3_16.pdf, consultato da ultimo in data 21 giugno 2022).

[117] I precedenti approcci, per citarne alcuni, erano basati sulla valutazione e gestione del rischio (*intelligence-led policing*, ILP), sui dati oggettivi (*data-driven policing*) o sulle "zone calde" (*hotspot policing*).

[118] Tradotto: «l'esplicita proiezione nel futuro». L. BENNETT MOSES – J. CHAN, *Algorithmic prediction in policing*, op. cit., p. 808.

[119] Cfr. M. MENDOLA, *One Step Further in the "Surveillance Society"*, op. cit., pp. 5-7; R. PELLICCIA, *Polizia Predittiva*, op. cit. p. 1; L. BENNETT MOSES – J. CHAN, *Algorithmic prediction in policing*, op. cit., p. 808.

I dispositivi di polizia predittiva – «siano essi assistiti o meno da sistemi di IA»[120] – si dividono sostanzialmente in due categorie:

> «- quelli che, ispirandosi alle acquisizioni della criminologia ambientale, individuano le c.d. "zone calde" (*hotspot*), vale a dire i luoghi che costituiscono il possibile scenario dell'eventuale futura commissione di determinati reati;
>
> - quelli che, ispirandosi invece all'idea del[la connessione criminale (*crime linking*)], seguono le serialità criminali di determinati soggetti (individuati o ancóra da individuare), per prevedere dove e quando costoro commetteranno il prossimo reato»[121].

Attraverso questi diversi approcci, le forze di polizia sono in grado di approntare vari metodi d'analisi volti ad individuare: luogo e tempo in cui è più probabile siano realizzati gli specifici crimini oggetto della statistica; il profilo dei possibili futuri criminali e del criminale potenzialmente unico autore di una serie di reati; gli individui o i gruppi sociali che potrebbero diventare vittime del crimine[122].

Come già indicato, la natura della polizia predittiva non va assolutamente confusa con quella del sistema Precrimine descritta in *Minority Report*. «*Predictive methods, themselves, may not expose sufficient probable cause to apprehend a suspected offender. "Predictions" are generated through statistical calculations that produce estimates, at best; like all techniques that extrapolate the future based on the past, they assume that the past is prologue. Consequently, the results are probabilistic, not certain*»[123]. Con la conoscenza del territorio e le informazioni che in esso vengono raccolte e la valutazione dei modelli comportamentali elaborati, le forze di polizia calcolano le probabilità che i criminali si comportino in un determinato modo, potenzialmente anticipandone così le mosse e prevenendo la commissione di un crimine. Questo perché i criminali tendono ad operare nelle zone in cui si sentono sicuri («*comfort zone*»), compiendo lo stesso tipo di crimine già commesso con successo in passato in identiche condizioni spaziali e temporali. Dunque, lo studio analitico delle circostanze permette di risalire a situazioni di rischio che hanno una più alta probabilità di accadimento con il fine ultimo di poter applicare i controlli laddove il rischio è attuale

---

[120] Così, F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 11. Essendo i dispositivi di polizia predittiva spesso coperti da segreto industriale, perché di proprietà privata, e comunque oggetto di segreto d'ufficio, visto il particolare compito al quale assolvono, i dettagli sulla loro progettazione non sono resi pubblici; non è chiaro quindi se, e in quale misura, i sistemi di IA siano alla base del loro funzionamento.

[121] *Idem*, p. 11; traduzione tra parentesi quadre mia. Analogamente, cfr. S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., p. 39; A. ZIROLDI, *Intelligenza artificiale e processo penale*, op. cit., p. 9.

[122] Cfr. W.L. PERRY – B. MCINNIS – C.C. PRICE – S.C. SMITH – J.S. HOLLYWOOD, *Predictive Policing*, op. cit., pp. 8-9.

[123] Tradotto: «I metodi predittivi, di per sé, potrebbero non svelare una probabile causa sufficiente per arrestare un sospettato di reato. Le "predizioni" sono generate attraverso calcoli statistici che producono, nella migliore delle ipotesi, stime; come tutte le tecniche che deducono il futuro in base al passato, presumono che il passato sia un prologo. Di conseguenza, i risultati sono probabilistici, non certi». W.L. PERRY – B. MCINNIS – C.C. PRICE – S.C. SMITH – J.S. HOLLYWOOD, *ult. cit.*, p. 8.

e più probabile.

Data questa impostazione, però, le categorie di reati sui quali si possono fornire previsioni sono limitate, perché i dispositivi di polizia predittiva necessitano di una gran mole di informazioni per funzionare e pochi e cattivi dati in entrata producono dati poco affidabili in uscita[124]: infatti, i limiti di questi strumenti si «mostrano […] in relazione ai reati di natura meno regolare o che colpiscono luoghi diversi, come gli atti di terrorismo»[125]. Per questo motivo, i reati ad oggi considerati e considerabili sono solo quelli caratterizzati da serialità[126], quali la rapina e lo spaccio di stupefacenti, ma nulla vieta di estenderne l'utilizzo verso altre condotte illecite[127] o eventi negativi[128], anche se non propriamente criminali, ferma restando la loro non sporadicità: in pratica, «maggiore è la lunghezza della serie, migliore è la capacità di previsione»[129] dell'algoritmo.

Generalizzando, il processo di predisposizione dell'intervento preventivo consiste in un ciclo continuo di attività, le cui fasi possono essere così descritte: raccolta di dati ed informazioni; analisi; intervento di polizia; risposta criminale, con conseguente modifica del contesto e necessaria nuova raccolta dati da parte delle forze di polizia[130].

La predizione – meglio, la previsione statistica o probabilistica – è il risultato dell'analisi semplice o complessa (quest'ultima frutto di fusione o interpolazione) di diversi tipi di dati, le cui quantità e qualità determinano l'utilità e l'efficacia dell'approccio preventivo tentato. Tra i dati

---

[124] Stando al vecchio adagio anglosassone "*garbage in, garbage out*" ("immondizia dentro, immondizia fuori"), se si riempie un *software* di analisi con dati errati, si otterranno risultati sbagliati.

[125] Così, X. RONSIN – V. LAMPOS (a cura di), *Appendice I*, cit., Punto 121, p. 35.

[126] Cfr., G. MASTROBUONI, *Crime is Terribly Revealing: Information Technology and Police Productivity*, in *Review of Economic Studies*, vol. 87, n. 6/2020, pp. 2727-2753 (edito nel 2014, ma pubblicato *online* il 7 marzo 2020 e reperibile al collegamento https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2989914, consultato da ultimo in data 21 giugno 2022) con uno studio riferito allo specifico programma italiano Keycrime, utilizzato dalla Questura di Milano. La necessità per i dispositivi di polizia predittiva di lavorare sulla serialità degli eventi per operare efficacemente è comunque generale e non riferibile solo a specifici algoritmi.

[127] I programmi possono essere adattabili a contrastare le truffe agli anziani, i furti o le violenze carnali, «atteso che il "meccanismo" di funzionamento può essere sostanzialmente identico». Così, cfr. C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 57, in riferimento alla duttilità dello specifico programma Keycrime.

[128] La Polizia Locale del Comune di Caorle, nel veneziano, si avvale per la sicurezza urbana dal maggio 2021 dell'algoritmo di polizia predittiva PELTA Suite, che pare prestarsi alla personalizzazione degli eventi negativi – qui nei limiti delle competenze comunali – che si intendono contrastare, quali l'abbandono di rifiuti, il disturbo causato da rumori molesti, gli abusi commerciali, gli incidenti stradali e, in un contesto di emergenza sanitaria da COVID-19, i comportamenti in violazione delle regole anti-contagio. Per la presentazione dell'algoritmo PELTA Suite, si veda il sito https://www.pelta.it/, consultato da ultimo in data 21 giugno 2022. Il *software*, sviluppato dalla società XServizi, elabora sia i dati di ciò che è avvenuto in passato a Caorle sia le informazioni che circolano in Rete, arrivando a prevedere un possibile evento negativo con – sostiene Angelo Russo, Direttore della Sicurezza della società sviluppatrice – «un'affidabilità predittiva di oltre il 90 per cento». La notizia è stata riportata con un comunicato stampa nel sito istituzionale del Comune di Caorle (reperibile *online* al collegamento https://www.comune.caorle.ve.it/index.php?area=5&menu=292&page=1299&lingua=4&idnotizia=4086, consultato da ultimo in data 21 giugno 2022).

[129] Così R. PELLICCIA, *Polizia Predittiva*, op. cit. p. 3, che riporta le conclusioni dello studio condotto da Mastrobuoni sul programma Keycrime (v. *infra*).

[130] Cfr. W.L. PERRY – B. MCINNIS – C.C. PRICE – S.C. SMITH – J.S. HOLLYWOOD, *Predictive Policing*, op. cit., pp. 11-15. Per la descrizione dettagliata delle singole fasi, si veda L. BENNETT MOSES – J. CHAN, *Algorithmic prediction in policing*, op. cit., pp. 806-822.

raccolti ed oggetto di rielaborazione vi sono, tra i tanti, quelli relativi: «a notizie di reati precedentemente commessi, agli spostamenti e alle attività di soggetti sospettati, ai luoghi, teatro di ricorrenti azioni criminali, e alle caratteristiche di questi luoghi, al periodo dell'anno o alle condizioni atmosferiche maggiormente connesse alla commissione di determinati reati; […] talora […] all'origine etnica, al livello di scolarizzazione, alle condizioni economiche, alle caratteristiche somatiche (… una rivincita di Lombroso?), riconducibili a soggetti appartenenti a determinate categorie criminologiche (ad es., potenziali terroristi) […]»[131].

Lacune nella raccolta di dati, dovute, a seguito di un evento criminoso noto, alla mancata verbalizzazione in modo meticoloso delle informazioni necessarie o proprio alla mancata denuncia di quanto avvenuto da parte delle vittime, determinano l'impossibilità per i dispositivi di fare previsioni utili legate all'effettività della situazione[132]. Inoltre, c'è il rischio che previsioni viziate all'origine, ma frutto di un processo di elaborazione imparziale ed oggettivo di una macchina, non facciano altro che perpetuare situazioni di pregiudizio e discriminazione: infatti, la «*neutralité prônée par les autorités en faveur du développement de ces dispositifs est fallacieuse. […] Les préjugés, les discriminations et l'axiologie dominante ne s'en trouvent pas amoindris, mais renforcés par l'illusion de la neutralité de la machine*»[133]. Da ciò si possono trarre due considerazioni: in primo luogo, come già rilevato dal Parlamento Europeo nel 2017, «dati e/o procedure di scarsa qualità alla base dei processi decisionali e degli strumenti analitici potrebbero portare ad algoritmi [starati], correlazioni spurie, errori, sottostima delle implicazioni giuridiche, sociali ed etiche»[134]; in secondo luogo, l'accuratezza dell'algoritmo deve essere misurata indipendentemente dalla valutazione dei risultati ottenuti con il suo utilizzo.

In fase di raccolta ed analisi, questione delicata è quella della trattazione dei dati sensibili riferiti al criminale – ad esempio, l'etnia – perché potrebbero indurre gli algoritmi a causare discriminazioni. La scelta di impiegare o meno questi dati è controversa, ma la soluzione di evitarne completamente l'utilizzo appare semplicistica: infatti, «*removing all variables that correlate with*

---

[131] In questi termini, F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 10.

[132] Analogamente, W.L. PERRY – B. MCINNIS – C.C. PRICE – S.C. SMITH – J.S. HOLLYWOOD, *Predictive Policing*, op. cit., p. 13: «*All predictive policing techniques depend on data. Both the volume and the quality of these data will determine the usefulness of any approach*» (tradotto: «Tutte le tecniche di polizia predittiva dipendono dai dati. Sia il volume sia la qualità di questi dati determineranno l'utilità di qualsiasi approccio»).

[133] Tradotto: «[La] neutralità sbandierata dalla autorità in favore dello sviluppo di tali dispositivi è fallace. […] I pregiudizi, le discriminazioni e l'assiologia dominante non sono diminuiti, ma rafforzati dall'illusione della neutralità della macchina». M. COORTEL, *Prospecter et punir: étude critique des logiciels Blue Crush et PredPol*, in *Encyclo. Revue de l'ecole doctorale ED 382*, Université Sorbonne Paris Cité, n. 7/2015 (*Dossier thématique: Traces de la politique, politique des traces*), p. 82 (reperibile *online* al collegamento https://www.researchgate.net/publication/316015733_Prospecter_et_punir_etude_critique_des_logiciels_Blue_Crush_et_PredPol, consultato da ultimo in data 21 giugno 2022).

[134] Parlamento Europeo – Commissione per le libertà civili, la giustizia e gli affari interni (LIBE), *Relazione sulle implicazioni dei* Big Data *per i diritti fondamentali:* privacy*, protezione dei dati, non discriminazione, sicurezza e attività di contrasto*, 2016/2225(INI), 20 febbraio 2017, par. M. (reperibile *online* al collegamento https://www.europarl.europa.eu/doceo/document/A-8-2017-0044_IT.html, consultato da ultimo in data 21 giugno 2022).

sensitive variables would reduce predictive accuracy significantly to the point that predictive analytics becomes impossible»[135]. Il modo di ovviare a questa problematica è fare in modo che quell'informazione sia utilizzata dal *software* non in via predominante, con il risultato di causare un controllo indiscriminato verso tutti gli appartenenti a quella specifica categoria, ma affiancata a molte altre, così da permettere agli operatori di polizia di concentrarsi strettamente su persone che corrispondono al profilo ricercato. A ben vedere però, come si spiegherà meglio in seguito, la possibilità che il controllo di polizia verso determinati gruppi sociali o etnici sia avvertita come discriminatoria si pone maggiormente con i sistemi che individuano le zone più soggette ad attività criminale, piuttosto che con i dispositivi che ricercano determinati soggetti per il loro *modus operandi*.

Infine, una volta raccolti i dati ed analizzati, le forze di polizia calibrano le loro attività di controllo del territorio sulle previsioni ottenute con azioni di pattugliamento mirate, «aumenta[ndo] la percentuale di arresti in flagranza»[136] o ottenendo un effetto dissuasivo[137]. Di conseguenza, l'attività criminale non fermata o scoraggiata tenderà a migrare in altre zone e questo cambiamento determinerà la necessità di raccogliere nuovi dati per permettere al *software* di elaborare delle previsioni probabilistiche aggiornate.

2.2.1. Diverse sperimentazioni, molte insidie e alcune soluzioni

Diffusi soprattutto negli Stati Uniti d'America[138], gli strumenti di polizia predittiva sono stati sperimentati, con fortune alterne, anche in Europa[139] ed altri Paesi[140].

Per gli Stati Uniti, si può menzionare, tra i tanti[141], l'algoritmo PredPol[142], finalizzato alla

---

[135] Tradotto: «la rimozione di tutte le variabili correlate a dati sensibili ridurrebbe l'accuratezza predittiva significativamente, al punto che l'analisi predittiva diventa impossibile». L. BENNETT MOSES – J. CHAN, *Algorithmic prediction in policing*, op. cit., p. 812.

[136] Così, S. SIGNORATO, *Giustizia penale e intelligenza artificiale*, op. cit., p. 607.

[137] Cfr. W.L. PERRY – B. MCINNIS – C.C. PRICE – S.C. SMITH – J.S. HOLLYWOOD, *Predictive Policing*, op. cit., p. 15.

[138] Cfr. Police Executive Research Forum. 2014, *Future trends in policing*, Washington, D.C.: Office of Community Oriented Policing Services, 2014, p. 3 (reperibile *online* al collegamento https://www.policeforum.org/assets/docs/Free_Online_Documents/Leadership/future%20trends%20in%20policing%202014.pdf, consultato da ultimo in data 21 giugno 2022).

[139] Per il contesto del Regno Unito, si veda A. BABUTA – M. OSWALD, *Data Analytics and Algorithms in Policing in England and Wales*, Royal United Services Institute, London 2020 (reperibile *online* al collegamento https://researchportal.northumbria.ac.uk/ws/portalfiles/portal/27680384/rusi_pub_165_2020_01_algorithmic_policing_babuta_final_web_copy.pdf, consultato da ultimo in data 21 giugno 2022).

[140] Per un confronto tra vari algoritmi di polizia predittiva, si veda V. DI COSTANZO, *Report K-crime: prevedere il crimine dal Key-Crime a Palantir*, in www.salvisjuribus.it, 27 settembre 2020 (reperibile *online* al collegamento http://www.salvisjuribus.it/report-k-crime-prevedere-il-crimine-dal-key-crime-a-palantir/, consultato da ultimo in data 21 giugno 2022).

[141] Per una breve lista di altri algoritmi utilizzati negli USA, senza pretesa di esaustività, si vedano L. BENNETT MOSES – J. CHAN, *Algorithmic prediction in policing*, op. cit., p. 809 e C. CASTETS-RENARD – P. BESSE – J. LOUBES – L. PERRUSSEL, *Encadrement des risques techniques et juridiques*, op. cit., pp. 20-28. Tra questi, per citarne alcuni, vi sono Risk Terrain Modelling (RTM), Crime Risk Forecasting e Blue CRUSH (Criminal Reduction Utilizing Statistical

predizione di vari reati, dallo spaccio di stupefacenti in determinate aree urbane alle rapine, attraverso l'individuazione di zone calde.

Predpol, elaborato da alcuni ricercatori dell'Università della California di Los Angeles (UCLA) in collaborazione con il Dipartimento locale di polizia, è oggi venduto da un'azienda privata americana ed adottato da molti altri Dipartimenti di polizia. Se inizialmente la campagna pubblicitaria enfatizzava le percentuali di abbattimento del numero di crimini ottenuto in diverse località grazie al *software*[143], oggi essa punta decisamente a rassicurare la società sulla compatibilità dello stesso con i diritti civili e la *privacy*, piuttosto che a sottolineare la sua efficacia (che non viene dimenticata, ma appare in subordine). Queste le parole che si trovano nel sito dell'azienda: «*Predpol uses ONLY 3 data points – crime type, crime location, and crime date/time – to create its predictions. No personally identifiable information is ever used. No demographic, ethnic or socio-economic information is ever used. This eliminates the possibility for privacy or civil rights violations*»[144].

Un simile cambio di strategia può essere stato dettato dalle critiche avanzate da attivisti ed accademici, che da tempo denunciano il fatto che l'algoritmo – assieme ad altri dispositivi dal funzionamento simile – si presti ad un potenziale pregiudizio per alcune minoranze etniche e sociali, e dalla decisione di alcune amministrazioni locali di abbandonarne l'impiego proprio perché avrebbero riscontrato tale problema[145]. Nello specifico, nel 2016 lo Human Rights Data Analysis

---

History). Per la presentazione dell'algoritmo RTM, si veda il sito www.riskterrainmodeling.com, consultato da ultimo in data 21 giugno 2022. In argomento, si vedano, *ex multis*, J.M. CAPLAN – L.W. KENNEDY – J.D. BARNUM – E.L. PIZA, *Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis of Case Configurations to Explore the Dynamics of Criminogenic Behavior Settings*, in *Journal of Contemporary Criminal Justice*, vol. 33, n. 2/2017, pp. 133-151 (reperibile *online* al collegamento principale https://journals.sagepub.com/doi/10.1177/1043986216688814, oppure al collegamento secondario https://academicworks.cuny.edu/jj_pubs/179/, consultati da ultimo in data 21 giugno 2022); L.W. KENNEDY – M. DUGATO, *Forecasting Crime and Understanding its Causes. Applying Risk Terrain Modeling Worldwide*, in *European Journal on Criminal Policy and Research*, vol. 24, n. 4/2018, pp. 345-513 (reperibile *online* al collegamento https://link.springer.com/journal/10610/volumes-and-issues/24-4, consultato da ultimo in data 21 giugno 2022). Invece, per un'analisi dell'algoritmo Crime Risk Forecasting, si veda C. CASTETS-RENARD – P. BESSE – J. LOUBES – L. PERRUSSEL, *Encadrement des risques techniques et juridiques*, op. cit., pp. 20-23. Infine, per informazioni su Blue CRUSH, si vedano la descrizione nel sito dell'azienda produttrice IBM (reperibile *online* al collegamento https://www.ibm.com/ibm/history/ibm100/us/en/icons/crimefighting/, consultato da ultimo in data 21 giugno 2022) e M. COORTEL, *Prospecter et punir*, op. cit., pp. 65-83.

[142] Per la presentazione dell'algoritmo PredPol, si veda il sito www.predpol.com.

[143] Cfr. F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 12.

[144] Tradotto: «PredPol utilizza SOLO 3 tipologie di dati – tipo del reato, luogo del reato e data/ora del reato – per fare predizioni [previsioni]. Non è mai utilizzata alcuna informazione di identificazione personale. Non è mai utilizzata alcuna informazione demografica, etnica o socio-economica. Ciò elimina la possibilità che siano violate la *privacy* ed i diritti civili». La descrizione del *software* è reperibile al collegamento https://www.predpol.com/law-enforcement/, consultato da ultimo in data 21 giugno 2022.

[145] Ad esempio, il Dipartimento di Polizia di Oakland nel 2016 non ha rinnovato per i motivi detti la licenza per l'utilizzo di PredPol. Tim Birch, a capo dell'Ufficio ricerca e pianificazione del Dipartimento, dopo aver convinto l'amministrazione ad adottare il *software*, ha cambiato idea sulla sua utilità giungendo alla conclusione che «la città non aveva bisogno di dare alle persone un'altra ragione per essere sospettose. Era troppo facile per [loro] interpretare la polizia predittiva come un'altra forma di profilazione razziale. […] Forse avremmo potuto ridurre maggiormente il crimine utilizzando la polizia predittiva, ma le conseguenze inattese [gli effetti collaterali riscontrati] sono molti più dannosi». Notizie riferite da E. THOMAS, *Why Oakland Police Turned Down Predictive Policing*, in www.vice.com, 28

Group (HRDAG), confrontando le previsioni di PredPol sulla città di Oakland relative all'uso di droghe con i dati raccolti dal Censimento e dall'Indagine sulla salute ed il consumo di tabacco, alcol e droga[146], ha dimostrato che le zone segnalate dal *software* come maggiormente a rischio erano quelle abitate perlopiù da cittadini afro-americani con basso reddito, quando invece dall'Indagine risultava che l'uso illecito di sostanze stupefacenti fosse diffuso omogeneamente in tutta la città[147]. La discordanza tra le due fotografie sarebbe dovuta ai dati che il dispositivo utilizza per compiere l'attività di elaborazione: infatti, essendo forniti dati storici sulle denunce, questo sarebbe portato a dare previsioni sul comportamento delle vittime e della polizia, piuttosto che dei criminali[148]; dunque, «apprenderebbe e costruirebbe le sue previsioni sulla base dei pregiudizi radicati nella società»[149] racchiusi negli stessi dati, con la conseguenza che «*rather than correcting for the apparent biases in the police data, the model reinforces these biases*»[150]. Ad oggi, le critiche ai dispositivi in generale che individuano le zone calde, inizialmente limitate alla necessità di utilizzare dati neutri in luogo di «*dirty data*» (dati sporchi)[151], sono comunque arrivate al punto di mettere in discussione la bontà degli algoritmi in sé, in quanto darebbero risultati discriminatori proprio per mancanze sorte in fase di elaborazione e non solo per la cattiva qualità dei dati utilizzati[152].

---

dicembre 2016 (reperibile *online* al collegamento https://www.vice.com/en/article/ezp8zp/__minority-retort-why-oakland-police-turned-down-predictive-policing, consultato da ultimo in data 21 giugno 2022). Ora, a parere di chi scrive, questa disfunzione effettivamente si riscontra nei sistemi che individuano le zone calde, ma non è da considerarsi propria di tutti gli algoritmi di polizia predittiva. Bisogna evitare di vedere a priori in tutti questi dispositivi «un'altra forma di profilazione razziale» con i quali verrebbero ammantati di oggettività e neutralità quelli che invece sono pregiudizi radicati nella società. Questo accade perché i dati elaborati dai dispositivi non sono neutri e – cosa peggiore, che va direttamente ad inficiare la bontà dell'algoritmo in sé – l'algoritmo non è stato pensato per considerare alcuni fattori, come le condizioni socio-economiche delle persone e degli ambienti, che invece sono importanti nello studio del comportamento criminale (v. *infra*). Comunque, agli inizi del 2021 il Consiglio cittadino della città di Oakland ha emesso un'ordinanza con la quale, oltre a rinnovare il rifiuto di utilizzare gli strumenti di polizia predittiva, mette al bando anche i dispositivi di riconoscimento facciale impiegati nelle attività di sorveglianza (reperibile *online* al collegamento https://www.eff.org/files/2021/01/20/2021-01-12_-_oakland_surveillance_ordinance_as_presented_to_city_council.pdf, consultato da ultimo in data 21 giugno 2022).

[146] National Survey on Drug Use and Health (NSDUH).

[147] Cfr. K. LUM – W. ISAAC, *To predict and serve?*, in *Significance*, vol. 13, n. 5/2016, pp. 14-19 (reperibile *online* al collegamento https://rss.onlinelibrary.wiley.com/doi/epdf/10.1111/j.1740-9713.2016.00960.x, consultato da ultimo in data 21 giugno 2022). Il riferimento a questo ed altri articoli simili è riportato nel sito dell'organizzazione (https://hrdag.org/usa/, consultato da ultimo in data 21 giugno 2022) al paragrafo "*The Problem with Predictive Policing*".

[148] A causa di ciò, tali dispositivi si limiterebbero anche a rappresentare il passato, senza l'effettiva capacità di individuare nuove tendenze criminali.

[149] Così, R. PELLICCIA, *Polizia Predittiva*, op. cit. p. 3.

[150] Tradotto: «piuttosto che correggere gli evidenti pregiudizi [contenuti] nei dati della polizia, il modello rafforza questi pregiudizi». K. LUM – W. ISAAC, *To predict and serve?*, op. cit., p. 18.

[151] Cfr. R. RICHARDSON – J. SCHULTZ – K. CRAWFORD, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, in *New York University Law Review Online*, vol. 94, n. 15/2019, pp. 192-233 (reperibile *online* al collegamento https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf, consultato da ultimo in data 21 giugno 2022).

[152] Cfr. N. AKPINAR – M. DE-ARTEAGA – A. CHOULDECHOVA, *The effect of differential victim crime reporting on predictive policing systems*, in *FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and*

Come ulteriore risultato di tale impostazione, vi sarebbe il rischio di generare le c.d. profezie che si autoavverano (*self-fulfilling prophecies*), circoli viziosi che si producono per il fatto che le zone considerate a rischio attirerebbero più attenzione della polizia, la quale rileverebbe ancóra più criminalità, portando ad una militarizzazione delle zone più difficili ed al nascere di tensioni con le comunità lì residenti che si sentirebbero sorvegliate in modo sproporzionato e discriminatorio[153].

Infine, altri dubbi riguardano proprio «[la] logica manageriale della risposta alla criminalità fornita da tali strumenti predittivi, in cui l'analisi approfondita delle ragioni alla base del reato diviene meno importante rispetto all'intervento sul posto e immediato»[154]: infatti, prevedere statisticamente un delitto non permette di comprendere il motivo che spinge un individuo ad agire contro la legge.

In Francia, nel 2015 il Dipartimento ETALAB (in qualità di Direttore dei Dati dello Stato francese), incardinato nella Direzione Interministeriale del Sistema Digitale di Informazione e Comunicazione dello Stato Francese (DINSIC)[155], ha sviluppato in collaborazione con il Dipartimento della Sicurezza Nazionale Informatica e Sistemi (ST(SI)) PredVol, un algoritmo per la previsione dei furti legati ai veicoli. Lanciato nel 2016, dopo sei mesi di sperimentazione nel dipartimento dell'Oise, particolarmente esposto ai furti d'auto, la Gendarmeria[156] si è resa conto che le previsioni erano molto efficaci, ma non facevano che confermare le aree di rischio già note[157], con il risultato che il dispositivo «[*n'a pas apporté*] *d'information supplémentaire aux opérationnels*»[158]. L'algoritmo è stato quindi abbandonato in favore di Paved, un altro algoritmo sviluppato dalla Gendarmeria per scoraggiare tutti i tentativi d'effrazione.

Anche Paved non sta dando risultati soddisfacenti sul piano operativo[159], ma, utilizzando

---

Transparency, Association for Computing Machinery, New York 2021, pp. 838-849 (reperibile *online* al collegamento https://nakpinar.github.io/diff_victim_crime_rep.pdf, consultato da ultimo in data 21 giugno 2022). Dopo aver appreso i risultati di questa ricerca, l'avvocato Rashida Richardson, coautrice di *Dirty Data, Bad Predictions*, op. cit., ha abbandonato le sue posizioni volte a criticare l'utilizzo di «*dirty data*» nei dispositivi per sostenere la necessità di abbandonare completamente l'impiego dei dispositivi di polizia predittiva (cfr. intervista rilasciata a W.D. HEAVEN, *Predictive policing is still racist – whatever data it uses*, in www.technologyreview.com, 5 febbraio 2021, reperibile *online* al collegamento https://www.technologyreview.com/2021/02/05/1017560/predictive-policing-racist-algorithmic-bias-data-crime-predpol/, consultato da ultimo in data 21 giugno 2022).

[153] Cfr. R. PELLICCIA, *Polizia Predittiva*, op. cit. p. 4; F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 13; K. LUM – W. ISAAC, *To predict and serve?*, op. cit., pp. 18-19.

[154] Così, X. RONSIN – V. LAMPOS (a cura di), *Appendice I*, cit., Punto 123, p. 35.

[155] Dal 2019 al DINSIC è subentrata la Direzione Interministeriale Digitale (DINUM).

[156] La *Gendarmerie nationale* è incaricata del mantenimento dell'ordine nelle zone rurali ed extraurbane e del controllo delle frontiere, mentre la *Police nationale* opera nelle zone urbane.

[157] Cfr. F. GAUTHIER, *Prédire les vols de voitures?*, in www.etalab.gouv.fr, 12 gennaio 2018 (reperibile *online* al collegamento https://www.etalab.gouv.fr/predire-les-vols-de-voitures, consultato da ultimo in data 21 giugno 2022), quando afferma che «*l'essentiel de l'attention des patrouilles se dirigeait non pas sur les prédictions quotidiennes, mais sur la simple visualisation des faits passés*» (tradotto: «la maggior parte dell'attenzione delle pattuglie non era rivolta alle predizioni quotidiane, ma sulla semplice visualizzazione dei fatti passati»).

[158] Tradotto: «non apportava informazioni ulteriori al personale operativo». C. CASTETS-RENARD – P. BESSE – J. LOUBES – L. PERRUSSEL, *Encadrement des risques techniques et juridiques*, op. cit., p. 30.

[159] Cfr. *Idem*, p. 32.

dati previamente anonimizzati e provenienti dalle banche dati della Gendarmeria e della Polizia, pare assicurare il rispetto della *privacy* e fornire garanzie in termini sia di neutralità che di affidabilità dei dati utilizzati nell'elaborazione. L'anonimizzazione delle informazioni somministrate al *software* «*limite, par ailleurs, les risques en cas d'intrusion des systèmes ou de piratage des algorithmes*»[160].

Invece, in Germania – specificamente in Baviera – è utilizzato il dispositivo Precobs (Pre Crime Observation System), sviluppato nel 2011 dall'Institut für Musterbasierte Prognosetechnik[161], che cerca di prevenire effrazioni, rapine e furti d'auto. Visto il modello teorico su cui si basa, secondo il quale nel luogo in cui è stato registrato un crimine vi è la possibilità, nell'arco di qualche giorno che ne sia commesso un altro, Precobs sembra basarsi più sull'individuazione delle zone calde, piuttosto che sul modello della connessione criminale[162].

In considerazione delle circostanze per cui, visionati i risultati del *software*, l'ufficiale di polizia responsabile decide sempre se tenerne conto o scartarli e, «[a] parte le informazioni sulla scena del crimine, il sistema non utilizza alcun dato personale per fare previsioni sul crimine»[163], nel 2015 il Commissario statale bavarese per la Protezione dei dati ha dichiarato Precobs non in contrasto con le norme poste a tutela dei dati. Tuttavia, i critici di tale dispositivo ritengono – sulla scia di quanto già avvenuto in altri Paesi più o meno democratici[164] – che potrebbe facilmente

---

[160] Tradotto: «limita, inoltre, i rischi in caso di intrusione nel sistema o di hackeraggio agli algoritmi». *Idem*, p. 31.

[161] Per la presentazione dell'algoritmo Precobs, si veda il sito https://logobject.com/en/solutions/precobs-predictive-policing/, consultato da ultimo in data 21 giugno 2022.

[162] Di questo avviso anche A.D. SIGNORELLI, *Il software italiano che ha cambiato il mondo della polizia predittiva*, in www.wired.it, 18 maggio 2019 (reperibile *online* al collegamento https://www.wired.it/attualita/tech/2019/05/18/polizia-predittiva-software-italiano-keycrime/, consultato da ultimo in data 21 giugno 2022).

[163] Testo in lingua originale: «*Abgesehen von Angaben zum Tatort verwendet das System keine personenbezogenen Daten, um Tatvorhersagen zu treffen*». Comunicato stampa del Commissario statale bavarese per la Protezione dei dati, 2 novembre 2015 (reperibile *online* al collegamento https://www.datenschutz-bayern.de/presse/20150211_Precops.html, consultato da ultimo in data 21 giugno 2022). Comunque, i timori riportati nell'articolo non sono dovuti e riferiti all'effettiva attività dell'algoritmo in esame, quanto a potenziali usi strumentali e deviati che se ne potrebbero fare.

[164] Cfr. A. BONFANTI, Big data *e polizia predittiva*, op. cit., pp. 207-208, che riporta come in Danimarca siano state potenziate «le capacità di intrusione della polizia e dei servizi segreti nei dati personali, attraverso una piattaforma (POL-INTEL) che incrocia le banche dati della polizia […] con quelli acquisiti tramite videocamere, internet, social networks o ottenuti mediante *databrokers* […], realizzando in questo modo una collezione generalizzata di dati e informazioni senza limitazione di scopo». Sul tema, si veda J. LUND, *New Legal Framework for Predictive Policing in Denmark,* in www.edri.org, 22 febbraio 2017 (reperibile *online* al collegamento https://edri.org/our-work/new-legal-framework-for-predictive-policing-in-denmark/, consultato da ultimo in data 21 giugno 2022). Invece, in Cina i sistemi tecnologici per il mantenimento di sicurezza ed ordine pubblico sono più tarati sulla sorveglianza generalizzata dei cittadini, permettendo l'identificazione ed il controllo di persone potenzialmente pericolose: tra queste, oltre ai criminali, i dissidenti politici e tutti coloro che minano la stabilità del Paese. In argomento, Human Rights Watch, *China: Police "Big Data" Systems Violate Privacy, Target Dissent. Automated Systems Track People Authorities Claim "Threatening"*, in www.hrw.org, 19 novembre 2017 (reperibile *online* al collegamento https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent, consultato da ultimo in data 21 giugno 2022) e F. SCHAEFFER, *En Chine, 1,4 milliard de suspects sous surveillance*, in www.lesechos.fr, 6 giugno 2018 (reperibile *online* al collegamento https://www.lesechos.fr/2018/06/en-chine-14-milliard-de-suspects-sous-surveillance-991913, consultato da ultimo in data 21 giugno 2022). Infine, sullo specifico sistema cinese di Polizia Predittiva, si veda D. SPRICK, *Predictive Policing in China: An Authoritarian Dream of Public*

prestarsi a tecniche generalizzate di sorveglianza, vista la possibilità di utilizzare come fonti da cui trarre dati anche le piattaforme sociali e l'Internet delle Cose[165]: la questione, infatti, è capire quando e con quali limiti la raccolta di dati possa essere considerata giustificabile, in una società democratica.

La continua ed indiscriminata provvista di dati determina una compressione del diritto al rispetto della vita privata e di altri diritti fondamentali. «*It is precisely such scenarios against which data protection regulations and privacy as a fundamental right have been drafted*»[166]. Se non fossero comunque fissati dei principi guida alle operazioni di controllo eseguite dalla polizia in un momento normalmente non sottoposto a vincoli – come detto, per motivi di efficacia – come quello della prevenzione, attività che sembrerebbero meno lesive di quelle permesse e disciplinate nella fase di repressione risulterebbero in realtà più intrusive di queste ultime, determinando una significativa violazione dei diritti fondamentali[167].

Infine, il contesto italiano[168] sperimenta da anni i dispositivi XLAW[169] e KeyCrime[170], realizzati da due ex dipendenti della Polizia di Stato – Mario Venturi ed Elia Lombardo – sulla base dell'esperienza maturata direttamente sul campo della prevenzione. I due sistemi, sviluppati da aziende private, sono stati concessi in comodato d'uso[171], rispettivamente, alle Questure di

---

Security, in *Naveiñ Reet: Nordic Journal of Law and Social Research (NNJLSR),* n. 9/2019, pp. 299-324 (reperibile *online* al collegamento https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3700785, consultato da ultimo in data 21 giugno 2022): come rileva l'autore e come sopra già indicato, *«[i]t is […] to be expected that predictive policing in China will mainly be a more refined tool for the selective suppression of already targeted groups by the police and does not substantially reduce crime or increase overall security*» (tradotto: «c'è da aspettarsi che la polizia predittiva in Cina sarà principalmente uno strumento più raffinato per la selettiva soppressione di gruppi già sorvegliati dalla polizia e sostanzialmente non riduca il crimine o aumenti la sicurezza generale»); di conseguenza, nel sistema cinese di polizia predittiva non si possono trovare soluzioni democratiche e correttivi per mitigare le insidie – che, anzi, sono lì intensificate – che si celano dietro l'utilizzo poco accorto di questi algoritmi.

[165] Cfr. K. BIERMANN, *Noch hat niemand bewiesen, dass Data Mining der Polizei hilft*, in www.zeit.de, 29 marzo 2015, terza parte (reperibile *online* al collegamento https://www.zeit.de/digital/datenschutz/2015-03/predictive-policing-software-polizei-precobs, consultato da ultimo in data 21 giugno 2022).

[166] Tradotto: «È precisamente contro tali scenari che sono stati elaborati i regolamenti sulla protezione dei dati e la *privacy* come diritto fondamentale». J. KREMER, *The End of Freedom in Public Places?,* op. cit., p. 270.

[167] Cfr. *Idem*, p. 271.

[168] Per una breve panoramica sull'applicazione di dispositivi di polizia predittiva in Italia, si veda L. ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Diritto penale e processo*, n. 6/2021, pp. 724-734.

[169] Per la presentazione del dispositivo XLAW, si vedano il sito www.xlaw.it, consultato da ultimo in data 21 giugno 2022, e E. LOMBARDO, *Sicurezza 4P. Lo studio alla base del software XLAW per prevedere e prevenire i crimini*, Mazzanti Libri, Venezia 2019.

[170] Per la presentazione del dispositivo KeyCrime, si vedano il sito www.keycrime.com, consultato da ultimo in data 21 giugno 2022; M. VENTURI, *KeyCrime©. La chiave del crimine*, in *Profiling. I profili dell'abuso*, n. 4/2014 (reperibile *online* al collegamento https://www.onap-profiling.org/keycrime-la-chiave-del-crimine/, consultato da ultimo in data 21 giugno 2022); F. SANVITALE, *A Milano la polizia ha KeyCrime, il software che prevede i reati. E funziona.*, in www.cronaca-nera.it, 9 aprile 2015 (reperibile *online* al collegamento http://www.cronaca-nera.it/4038/milano-key-crime-software-prevede-reati, consultato da ultimo in data 21 giugno 2022); C. MORABITO, *La chiave del crimine*, in *Polizia Moderna*, luglio 2015, pp. 36-38 (reperibile *online* al collegamento https://www.poliziadistato.it/statics/16/la-chiave-del-crimine.pdf, consultato da ultimo in data 21 giugno 2022); A.D. SIGNORELLI, *Il software italiano*, op. cit; C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., pp. 56-59.

[171] In argomento, F. SANVITALE, *A Milano la polizia ha KeyCrime*, op. cit., ultimo capoverso; il sito aziendale di KeyCrime (https://keycrime.com/stampa4/, consultato da ultimo in data 21 giugno 2022); C. MORELLI, *Furti e rapine: a*

Napoli[172] e di Milano, che dai primi del 2000 ne sperimentano l'utilità contro i reati predatori e le rapine in ambito commerciale e bancario. Entrambi i dispositivi, ognuno per le sue caratteristiche, sembrano essere riusciti a superare le criticità sopra emerse, tanto da essere validati da ricerche universitarie ed Istituzioni[173]. L'opera di sviluppo dei sistemi è stata assistita fin dalle prime fasi, oltre che da ingegneri informatici, matematici e statistici, da sociologi, psicologi, criminologi ed urbanisti, con l'obiettivo di tradurre in codice le teorie criminologiche elaborate a partite dai modelli comportamentali costruiti con i dati empirici a disposizione durante la fase delle attività di polizia di tipo preventivo, per come sopra descritta.

Sull'opportunità di rendere i dispositivi trasparenti ed analizzabili dall'opinione pubblica, i due ideatori hanno opinioni diverse. Per quanto riguarda XLAW, addetti ai lavori e figure del mondo giuridico ed accademico hanno potuto verificare il funzionamento del dispositivo e contribuire in tal senso, realizzando così quel concetto di "*white box*" – concetto su cui tanto puntano le Carte etiche citate nell'indicare le linee guida per costruire strumenti di IA affidabili – per cui sia la società sia gli operatori che lavorano con tale strumentazione siano in grado di comprenderne il funzionamento, i limiti nell'elaborazione dei dati, ferma restando l'indiscutibile predominanza della decisione umana sul da farsi con le previsioni elaborate. Invece, su KeyCrime questa apertura non c'è stata per motivi legati al funzionamento dell'algoritmo ed all'organizzazione del sistema giuridico italiano: infatti, siccome il dispositivo è un tassello del processo investigativo che serve "solamente" a collegare crimini avvenuti in momenti diversi, prevedendo prossimi obiettivi, gli operatori di polizia non sono esentati dal decidere il da farsi e compiere le normali attività investigative e di raccolta delle prove per come previste dal normale *iter* procedimentale (in altre parole, il dispositivo non ha alcuna valenza scientifica in sede processuale)[174].

XLAW, basando la sua attività di rielaborazione sui dati estratti dalle denunce inoltrate alla

---

sventarli ci pensa l'intelligenza artificiale!, in www.altalex.com, 6 maggio 2019, paragrafo "XLAW" (reperibile *online* al collegamento https://www.altalex.com/documents/news/2019/05/06/polizia-predittiva-intelligenza-artificiale, consultato da ultimo in data 21 giugno 2022).

[172] XLAW è ora adottato non più solo a Napoli, ma in varie città: Prato, Salerno, Venezia, Modena e Parma. Nel sito di XLAW sono raccolti tutti gli spazi informativi – da articoli di giornale a servizi video – dedicati all'utilizzo del *software* nei vari capoluoghi (https://www.xlaw.it/presentazione/, consultato da ultimo in data 21 giugno 2022).

[173] Il dispositivo XLAW è stato validato dall'Università Federico II di Napoli e dalla Direzione Centrale Anticrimine del Ministero dell'Interno – Dipartimento di Pubblica Sicurezza. Per validazione universitaria, si veda G. DI GENNARO – E. LOMBARDO – R. MARSELLI – M. SPINA, *Tolleranza zero o deterrenza selettiva: quali strade intraprendere per rispondere più efficacemente alla domanda di sicurezza*, in G. DI GENNARO – R. MARSELLI (a cura di), *Secondo Rapporto – Criminalità e Sicurezza a Napoli*, Federico II University Press, Napoli 2017, pp. 197-204 (reperibile *online* al collegamento http://www.fedoa.unina.it/11938/, consultato da ultimo in data 21 giugno 2022). Invece, il dispositivo KeyCrime è stato validato da uno studio condotto dall'Università di Essex in tema "*Impact: Imagine being able to predict a crime in the future*" (https://www.essex.ac.uk/research/showcase/imagine-being-able-to-predict-a-crime-in-the-future, consultato da ultimo in data 21 giugno 2022); i risultati della ricerca sono stati riportati in G. MASTROBUONI, *Crime is Terribly Revealing*, op. cit.

[174] Cfr. A.D. SIGNORELLI, *Il software italiano*, op. cit., ultimo capoverso.

Polizia di Stato, dalle informazioni della Polizia locale e sulle indicazioni di chi vive in determinate zone, lavora con un algoritmo euristico (non statistico), cioè su base probabilistica, per individuare, all'interno di "riserve di caccia"[175] con peculiari caratteristiche e dinamiche socio-economiche, il processo ciclico ed il momento di reiterazione del reato, da parte di un singolo o gruppo criminale, in determinati orari e momenti[176]. Come detto, i sistemi che ricercano le zone calde sono molto criticati perché riprodurrebbero pregiudizi e storture contenuti nei dati loro forniti; dati riferiti solo alle percezioni ed ai comportamenti di vittime e forze di polizia e per nulla riguardanti i criminali e le condizioni sociali e strutturali nel quale e dal quale operano[177]. Altre condizioni sono state, invece, messe al centro dell'elaborazione dell'algoritmo di XLAW, anche per il fatto stesso di non basarsi sulla classica individuazione di zone calde; in questo modo, non ci si concentra solo sul reo, ma si realizzano modellazioni che tengono conto dell'aspetto soggettivo e del contesto, con tutte le condizioni, fasi e operazioni di tipo sociale, economico e urbanistico che vi si trovano all'interno, le tipologie di vittime e gli obiettivi coinvolti, il giorno, l'ora, la stagione ed altro. XLAW, quindi, ha un'impostazione *sui generis*, in quanto prevede il comportamento e le mosse di un generico criminale in relazione alle dinamiche che avvengono in determinate zone.

La soluzione adottata[178] descrive il tipo di reato, il *modus operandi* dell'autore e l'obiettivo, ed indica agli operatori di polizia i luoghi e gli orari precisi in cui si potrà consumare un crimine, consentendo così loro di predisporre una mirata attività di pattugliamento per impedire la commissione di tali reati e cogliere in flagranza i potenziali autori degli stessi.

Il sistema KeyCrime, invece, basandosi sul modello del collegamento criminale (*crime linking*), cerca di capire quali crimini vengono compiuti dagli stessi rapinatori (astrae dunque la serie criminale) per prevedere dove, come e quando questi stessi rapinatori compiranno la prossima

---

[175] Le riserve di caccia sono aree in cui vi è la possibilità di commettere un reato predatorio più volte nel tempo, in maniera regolamentata. Queste aree sono redditizie, sono sicure e vi è la mancanza di un controllo adeguato. All'interno delle Riserve di Caccia esistono precise regole, che sono indotte dalla costanza dei fattori presenti e pertanto all'interno delle stesse vi è un ordine costante, ripetutamente verificato, di una serie di eventi. La riserva di caccia è frutto della rivisitazione del concetto di *hot spot*, in quanto non vi sarebbe correlazione tra concentrazione di reati predatori e fattori ambientali (es. Teoria delle finestre rotte) e tra criminalità e fattori sociali e strutturali. Cfr. E. LOMBARDO, *Sicurezza 4P*, op. cit. Il Sistema XLAW si basa, appunto, sulle 4 "P": prevenzione, previsione, proattività e partecipazione.

[176] Cfr. G. CRUPI, *XLAW – Innovazione strategica e tecnologica per la prevenzione dei reati predatori urbani*, in *Polizia – Periodico S.I.A.P.*, n. 69/2018, pp. 59-63 (reperibile *online* al collegamento https://www.siap-polizia.org/media/94/74368506459767/polizia_69_web162333.pdf, consultato da ultimo in data 21 giugno 2022). In altre parole, il sistema sovrappone i crimini a queste dinamiche socio-economiche, estraendo sequenze e avvenimenti in concomitanza di queste fasi ed operazioni regolari.

[177] Cfr. R. RICHARDSON – J. SCHULTZ – K. CRAWFORD, *Dirty Data, Bad Predictions,* op. cit, pp. 225-227. L'avvocato Rashida Richardson – criticando i sistemi che individuano le zone calde, predominanti negli USA – ha affermato che «molti fornitori […] non capisc[o]no fondamentalmente quanto le condizioni strutturali e sociali influenz[a]no o distorc[o]no molte forme di dati sulla criminalità» (intervista del 5 febbraio 2021 al *MIT Technology Review* reperibile *online* al collegamento https://www.osce.org/it/chairmanship/454579, consultato da ultimo in data 21 giugno 2022).

[178] Allo stesso modo funziona l'algoritmo PELTA Suite, già citato, che si basa sulla logica che numerosi eventi hanno caratteristiche di ciclicità e stanzialità.

azione[179]. Dunque, l'applicativo è «strutturato per una duplice finalità (polizia di prevenzione-polizia giudiziaria) e in grado di sfruttare in maniera sinergica il patrimonio cognitivo con il quale viene implementato»[180]. «Per farlo, il software struttura la raccolta di informazioni sulla base di interviste effettuate ad hoc, elaborate con l'aiuto di alcuni psicologi, per cogliere eventuali sfumature di comportamento dell'autore con un notevole grado di dettaglio – [dove si sono compiute le rapine, a che ora, in che modo, come si sono comportanti i criminali, che mezzi ed armi hanno usato, come erano vestiti ed altro ancóra] – al fine di individuarne lo schema d'azione e prevedere, con la maggiore approssimazione possibile, dove e quando quello specifico soggetto colpirà di nuovo. L'obiettivo del software quindi non è quello di portare la polizia a presidiare un'area in cui è probabile che avvenga un crimine, ma di prevedere dove colpirà il criminale che si sta cercando»[181].

Di conseguenza, non si verificano né una criminalizzazione-militarizzazione delle aree, né discriminazioni contro soggetti appartenenti a fasce sociali deboli o a minoranze etniche, in quanto le forze di polizia ricercheranno solo gli individui corrispondenti al profilo indicato e non faranno controlli indiscriminati[182]. La persona o il gruppo ricercato è quindi già individuato, anche se non identificato. Come è stato osservato, lo «strumento *Keycrime* [… ,] lungi dall'utilizzare meri sistemi di emergenza statistica e modelli di raccolta di dati indiretti o a secchio[, come invece avviene nei modelli di polizia preventiva del tipo *hotspots*], si propone di valutare il rischio di recidivanza specifica in relazione ad una determinata serie criminale e lo fa sulla base di dati quanto mai diretti ed oggettivi, in una fase in cui il momento della valutazione giudiziaria è ancóra ben lontano»[183].

Punti di forza di KeyCrime sono i risultati raggiunti circa la capacità di risposta delle forze di polizia[184], la capacità di interfacciarsi con altre banche dati della Polizia (AFIS e SDI[185]), il suo

---

[179] Il sistema propone una serie di eventi che sono potenzialmente collegabili con quello appena inserito. Questa procedura permette di collegare tra loro dei reati che altrimenti potrebbero rimanere fatti singoli e a sé stanti sui quali sarebbe difficile, se non impossibile, indagare. La serie criminale così isolata, identificati i tratti comportamentali del criminale, consente di avere capacità predittive con ottime probabilità di successo.

[180] Così, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 56.

[181] In questi termini, R. PELLICCIA, *Polizia Predittiva*, op. cit. p. 3.

[182] Proprio per individuare la persona ricercata, KeyCrime, a differenza di altri sistemi, tiene conto anche dei dati relativi all'etnia del criminale. Quest'ultima è solo una delle tante caratteristiche dell'obiettivo degli operatori di polizia.

[183] Così, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 70.

[184] Cfr. G. MASTROBUONI, *Crime is Terribly Revealing*, op. cit., pp. 40-41, che però non manca di sollevare parallelamente dei dubbi: «*[a]n open question is whether over time, as criminals perceive the productivity of policing to be increasing, additional deterrence is generated. It could either deter crime altogether, convincing criminals to switch to other crimes, or it might displace crime from Milan to other cities. Criminals may also exert more effort to try to be more unpredictable. Another open question is whether the Polizia is using the best possible prediction algorithm and whether predictions could be improved using more or even less detail about the robberies*» (tradotto: «[u]na domanda aperta è se nel tempo, poiché i criminali percepiscono un aumento dell'efficienza della polizia, si genera ulteriore deterrenza. Questa potrebbe scoraggiare del tutto il crimine, convincere i criminali a passare ad altri reati, oppure determinare lo spostamento della criminalità da Milano ad altre città. I criminali potrebbero anche fare più sforzi per cercare di essere più imprevedibili. Un'altra questione aperta è se la Polizia stia utilizzando il miglior algoritmo di predizione possibile e se le previsioni potrebbero essere migliorate utilizzando più o anche meno dettagli sulle rapine»).

[185] L'AFIS (Automated Fingerprint Identification System) è il Sistema Automatizzato di Identificazione delle

utilizzo congiunto da parte di Polizia di Stato e Carabinieri e la possibilità di imputare al soggetto arrestato o fermato «non solo l'ultimo reato commesso (in occasione del quale egli è stato individuato), ma anche i precedenti reati costituenti la serie criminale ricostruita grazie all'archiviazione e all'elaborazione dei dati»[186].

Ora, riferendosi ad entrambi gli applicativi, «occorre chiedersi se [i] meccanism[i] descritt[i] possa[no] in qualche modo determinare una "compromissione" dei diritti dei soggetti che vengono individuati con tali modalità. In chiave di polizia di prevenzione, il programma potrà rivelarsi non efficace (o non sufficientemente efficace) ma indubbiamente non potrà definirsi non calibrato (anche in termini di proporzionalità della tecnica utilizzata) rispetto all'obiettivo. Se il soggetto – ancóra anonimo – individuato dall'analisi di una "serie" criminale [o ciclica] si presenta davanti a un ufficio postale con un coltello in tasca e si appresta a entrare nei locali, sussistono tutti gli elementi per avviare un procedimento nei suoi confronti. Il "coefficiente" di valutazione (e quindi la necessità di verificare la qualità e le forme del meccanismo di valutazione) è sostanzialmente inesistente, essendo l'esito dell'utilizzo direttamente apprezzabile»[187].

2.2.2 La compatibilità delle attività di polizia predittiva con i diritti fondamentali

L'analisi svolta su questi diversi algoritmi di polizia predittiva testimonia quali insidie si nascondono dietro il loro utilizzo e segnalare i tentativi e gli accorgimenti adottati per porvi rimedio. Si tratta di problematiche traversali che non vanno ricondotte solo allo specifico *softwar*e nel contesto del quale sono state sollevate; di certo, la bontà (in termini di efficacia) e la capacità di rispettare i diritti fondamentali del singolo algoritmo dipendono dalla qualità dei dati utilizzati e da scelte ed accorgimenti etici e tecnici presi durante la fase di sviluppo dei dispositivi stessi[188]. D'altra parte, però, ciò si traduce nell'impossibilità di fare valutazioni onnicomprensive sulla compatibilità o meno di questi sistemi con gli ordinamenti giuridici, rendendosi invece necessario procedere secondo un approccio caso per caso. Infine, il fatto che specifiche questioni siano accostate ad un certo dispositivo dipende anche dalla diversa risonanza mediatica che hanno nella società in cui lo stesso è utilizzato; non bisogna dimenticare, infatti, come l'ambito della polizia predittiva si intersechi anche con la criminologia e la sociologia, oltre che con il diritto penale[189]. È per questo motivo, ad esempio, che nel contesto statunitense trova più spazio la discussione sui rischi di

---

Impronte. Invece, lo SDI (Sistema di Indagine) permette la catalogazione delle informazioni acquisite dalle forze di polizia nel corso delle attività amministrative e delle attività di prevenzione e repressione dei reati e trasmesse al CED (Centro Elaborazione Dati), istituito dall'art. 8, L. 121/1981 e gestito dal Dipartimento della Pubblica Sicurezza.

[186] In questi termini, F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 13.

[187] Così, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., pp. 57-58.

[188] Cfr. A. ZIROLDI, *Intelligenza artificiale e processo penale*, op. cit., p. 8.

[189] Cfr. S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., p. 40.

discriminazione per certi gruppi etnici e sociali e sulla decisione di investire risorse in questi dispositivi repressivi piuttosto che ridurre il crimine agendo sui fattori criminogeni (fattori sociali, economici, ambientali, ecc.), mentre in quello europeo l'attenzione cade più sulla necessità di tutelare la *privacy*, i dati personali ed i diritti fondamentali. Tutti questi aspetti sono comunque sempre considerati nei diversi contesti di studio, ma appunto secondo un ordine di importanza e con sfaccettature differenti.

L'utilizzo dei dispositivi di polizia predittiva non risulta essere stato regolato, in nessun Paese, con una specifica disciplina normativa. Tuttavia, le attività di prevenzione delle forze di polizia – tralasciando quelle attuate dalle Agenzie di sicurezza – possono violare i diritti fondamentali delle persone, se l'utilizzo degli apparati predittivi, andando oltre l'obiettivo di prevenire attività criminali già in atto, diventa strumento per la sorveglianza di massa della società. L'uso abusivo, sproporzionato e non giustificato degli applicativi darebbe sicuramente forma ad un sistema orwelliano di sorveglianza e ciò si potrebbe tradurre nella violazione del diritto all'integrità psichica della persona (art. 3, Carta dei diritti fondamentali dell'UE o Carta di Nizza), del diritto alla libertà (art. 6, Carta di Nizza, ed art. 5, CEDU), del principio della presunzione di innocenza (art. 6, par. 2, CEDU), del diritto al rispetto della vita familiare e privata, del suo domicilio e delle sue comunicazioni (art. 7, Carta di Nizza, ed art. 8, CEDU), al diritto alla protezione dei dati personali (art. 8, Carta di Nizza), del diritto alla libertà di riunione ed associazione (art. 12, Carta di Nizza, ed art. 11, CEDU), del diritto all'uguaglianza ed alla non discriminazione (artt. 20-21, Carta di Nizza ed art. 14, CEDU).

In genere, l'utilizzo di *big data*[190] comporta rischi per la tutela della *privacy* e la protezione dei dati personali, in quanto i dati processati potrebbero non essere anonimi o essere facilmente ricondotti a soggetti individuati. Se il problema, in prima battuta, viene spesso associato al campo commerciale, anche nell'ambito della pubblica sicurezza si stanno ponendo gli stessi quesiti: infatti, come visto, alcuni dispositivi di polizia predittiva, oltre ai dati già in possesso delle forze di polizia, processano anche quelli acquisiti tramite videocamere[191] ed Internet, oppure ottenuti mediante

[190] «[I] Big Data si riferiscono alla raccolta, all'analisi e all'accumulo ricorrente di ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di un trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento dei dati, che usano sia informazioni memorizzate sia in streaming, al fine di individuare determinate correlazioni, tendenze e modelli (analisi dei Big Data)». Così, Parlamento Europeo, *Relazione sulle implicazioni dei* Big Data *per i diritti fondamentali*, op. cit., Considerando A.

[191] Il Ministero dell'Interno – Dipartimento di pubblica sicurezza aveva bandito nel 2017 una procedura volta alla fornitura di una soluzione per l'allestimento di un Sistema Automatico di Riconoscimento d'Immagini (SARI), volto a gestire due diversi scenari operativi. Da un lato, il sistema (versione SARI Enterprise) doveva essere in grado di ricercare un volto presente in un'immagine in modo automatico, per mezzo di algoritmi di riconoscimento facciale, all'interno dell'AFIS, una banca dati di soggetti fotosegnalati. Dall'altro, il sistema (versione SARI Real Time), impiegando i dati raccolti nello scenario *enterprise*, doveva analizzare in tempo reale i volti dei soggetti ripresi da telecamere installate in un'area geografica circoscritta e delineata, per poi confrontarli con i dati presenti in una banca dati ristretta e predefinita denominata "*watch-list*" (della grandezza dell'ordine di migliaia di immagini), con generazione di una segnalazione per gli operatori in caso di confronto positivo. Con riferimento al primo scenario, il

databrokers (*open source collection* e *social network analysis*).

Per regolamentare queste pratiche ed indicare un confine di liceità, nel contesto dell'Unione europea sono stati adottati, rispettivamente, il Regolamento (UE) n. 2016/679 sulla protezione dei dati (GDPR) e la Direttiva (UE) n. 2016/680[192].

Anzitutto, di fronte all'attività di raccolta generalizzata di dati, la Direttiva (UE) n. 2016/680, il GDPR e la CEDU prevedono dei casi nei quali il diritto alla *privacy* e della protezione dei dati personali possono essere limitati per esigenze di pubblica sicurezza[193].

La Direttiva, premesso che rimangono escluse dal suo ambito di regolazione le informazioni anonime, cioè le «informazioni che non si riferiscono a una persona fisica identificata o identificabile o [… i] dati personali resi sufficientemente anonimi da non consentire più l'identificazione dell'interessato»[194], autorizza gli Stati membri ad adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato, il diritto di questi

---

Garante della Privacy – con provvedimento n. 440/2018 – ha osservato che il trattamento di dati personali realizzato tramite SARI Enterprise non presenta criticità sotto un profilo di *privacy* (provvedimento reperibile *online* al collegamento https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9040256, consultato da ultimo in data 21 giugno 2022). Invece, per il secondo scenario il Garante – con parere n. 127/2021 – ha affermato che SARI Real Time non è conforme alla normativa sulla *privacy* perché, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale, non vi sarebbe una base normativa che giustificherebbe un tale trattamento dei dati biometrici (provvedimento reperibile *online* al collegamento https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877, consultato da ultimo in data 21 giugno 2022). Sul punto, si veda anche il comunicato stampa dello stesso Garante del 16 aprile 2021 (reperibile *online* al collegamento https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842, consultato da ultimo in data 21 giugno 2022). Per un commento sulle vicende del SARI e sui provvedimenti del Garante, si veda A. FONSI, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in www.penaledp.it, 14 maggio 2021 (reperibile *online* al collegamento https://www.penaledp.it/prevenzione-dei-reati-e-riconoscimento-facciale-il-parere-sfavorevole-del-garante-privacy-sul-sistema-sari-real-time/#_ftn3, consultato da ultimo in data 21 giugno 2022). Sui sistemi di riconoscimento facciale utilizzabili al riguardo in Italia e in Europa, si veda M. PISATI, *Indagini preliminari e intelligenza artificiale: efficienza e rischi per i diritti fondamentali*, in *Processo penale e giustizia*, fasc. n. 4/2020, p. 960; per rilievi critici in proposito (come i rischi di discriminazione di tipo razziale già sollevati nei confronti del dispositivo COMPAS), anche se precedente al parere n. 127/2021 del Garante Privacy, si veda J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice, in *Diritto Penale Contemporaneo*, n. 1/2020, pp. 242 e ss. (reperibile *online* al collegamento https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_1_2020_Della%20torre.pdf, consultato da ultimo in data 21 giugno 2022); M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Diritto penale e processo*, n. 8/2021, specificamente pp. 1048-1054.

[192] Nell'ordinamento italiano, la Direttiva è stata recepita con il D.Lgs. 51/2018. Il Decreto prevede una serie di diritti e tutele mutuati dal sistema "privacy": diritto di informazione, di accesso, di rettifica, di cancellazione; diritti da far valere, in caso di diniego non motivato, davanti al Garante della Privacy con la presentazione di un reclamo. Dove, però, la competenza del Garante è costretta a fermarsi è il procedimento penale: infatti, se il trattamento viene effettuato da una autorità giudiziaria, cade la tutela amministrativa e viene in primo piano solo quella endo-procedimentale penale per ragioni di tutela delle indagini e dell'andamento del processo. In questo contesto, in caso di presunte violazioni nel trattamento dei propri dati, l'interessato potrà avvalersi degli strumenti che corredano il diritto di difesa (artt. 116 e 130, c.p.p.).

[193] La Direttiva pare adottare un approccio equilibrato al tema del rapporto tra *privacy* e sicurezza, in quanto prevede che ci possano essere delle restrizioni alla *privacy* per esigenze sicuritarie, salvo che queste avvengano nel limite dello stretto necessario. Cfr. art. 4, co. 1, lett. c) e e).

[194] Direttiva (UE) 2016/680, Considerando 21. Si precisa che per, stabilire l'identificabilità di una persona fisica, devono essere presi in considerazione tutti i mezzi tecnologici di cui il titolare del trattamento o un terzo può avvalersi – in relazione anche ai costi ed al tempo necessario – per identificare direttamente o indirettamente detta persona.

di accedere ai suoi dati personali, di rettificarli o di richiederne la cancellazione[195], se e per il tempo in cui ciò costituisca «una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di: a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui»[196]. Analogamente, l'art. 23 GDPR ammette limitazioni ai vari diritti riconosciuti[197], purché le stesse «rispetti[no] l'essenza dei diritti e delle libertà fondamentali e sia[no] una misura necessaria e proporzionata in una società democratica» per assicurare, tra le tante materie indicate, la sicurezza nazionale e pubblica (co. 1, lett. a) e c)) e la prevenzione, l'indagine, l'accertamento e il perseguimento di reati (co. 1, lett. d), prima parte). Segue lo stesso orientamento anche la CEDU, che, all'art. 8, par. 2, ammette l'ingerenza di un'autorità pubblica nel diritto al rispetto della vita privata e familiare quando l'intromissione «sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, […] alla difesa dell'ordine e alla prevenzione dei reati, […] o alla protezione dei diritti e delle libertà altrui».

All'interno di queste deroghe, tuttavia, è necessario adottare degli accorgimenti volti a minimizzare – se non proprio ad evitare – il rischio di effetti distorsivi. Non a caso, lo stesso art. 8 Carta dei diritti fondamentali dell'UE, nello stabilire che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (co. 1), già a partire dal momento della raccolta[198], afferma che 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» (co. 2, prima parte).

Di conseguenza, il titolare del trattamento – ossia l'autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvaguardia contro e prevenzione di minacce alla pubblica sicurezza[199] – che si trovi a trattare «informazioni relative a una persona fisica identificata o identificabile»[200] dovrà, ai sensi dell'art. 20, par. 1 della Direttiva[201], predisporre «misure tecniche e organizzative adeguate, quali la

[195] Cfr. Direttiva (UE) 2016/680, Considerando 44 e 47.
[196] *Idem*, art. 15, co. 1.
[197] Le limitazioni possono riguardare i diritti di cui agli artt. 12-22 e 34, GDPR.
[198] Cfr. G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, op. cit., p. 79.
[199] Non si fa riferimento alle Agenzie occupate in questioni connesse alla sicurezza nazionale, la cui attività di raccolta dati non risulta quindi vincolata alla Direttiva (UE) 2016/680. Cfr. Considerando 14.
[200] Direttiva (UE) 2016/680, Considerando 21.
[201] Recepito nell'art. 16, co. 1, D.Lgs. 51/2018.

pseudonimizzazione[202],» volte a proteggere i dati e ad integrare le necessarie garanzie[203]. Anche se un dato personale oggetto di pseudonimizzazione non dovrebbe più essere attribuibile ad una persona specifica, si segnala che allo stato questo trattamento «non garantisce in modo assoluto e definitivo l'anonimato dei dati personali»[204], in quanto, grazie a tecniche di triangolazione, rimane possibile la reidentificazione[205]. Inoltre, il titolare del trattamento avrà l'obbligo di attuare «misure tecniche e organizzative adeguate [a] garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, tali misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica» (art. 20, par. 2)[206].

Pertanto, la protezione dei dati personali va prevista non solo nella fase del trattamento per impostazione predefinita (c.d. *privacy by default*), ma anche nella prodromica fase di programmazione del sistema di trattamento (*privacy by design*).

Il titolare del trattamento dovrà anche fare una valutazione dell'impatto che il trattamento – per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità – avrà sulla protezione dei dati personali, quando questo presenti un rischio elevato per i diritti e le libertà delle persone (art. 27, par. 1)[207].

Per quanto riguarda l'ambito nazionale, in materia è stato emanato, a norma dell'art. 57 Codice Privacy, il D.P.R. 15/2018, cioè il Regolamento sul trattamento dei dati personali da parte delle forze di polizia nell'esercizio dei compiti di prevenzione dei reati, tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria. Nell'ambito di tali interventi, sono disciplinati specifici termini di conservazione dei dati, differenziati in base al tipo di provvedimento adottato (art. 10, co. 3). Per quanto riguarda le specifiche attività di polizia predittiva, i dati relativi ad attività di indagine o polizia giudiziaria che non hanno dato luogo a procedimento penale possono essere conservati fino a 15 anni dall'ultimo trattamento (lett. i)); i dati relativi ad attività di

[202] La pseudonimizzazione è «il trattamento dei dati personali in modo tale che [gli stessi] non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile». Così, *Idem*, art. 3, par. 5.

[203] Per esempio, i produttori dell'algoritmo di polizia predittiva PELTA Suite, già citato, affermano che il loro prodotto rispetta la *privacy* perché si sono «imposti regole etiche ferree come la raccolta e l'analisi solo di dati anonimi e quindi di alcun dato sensibile relativo a cose e/o persone, una scelta che rende la soluzione in tutti i suoi aspetti "privacy by design" e "privacy by default"» (https://www.pelta.it/pelta-suite-sicurezza-urbana/, consultato da ultimo in data 21 giugno 2022).

[204] Così, A. BONFANTI, Big data *e polizia predittiva*, op. cit., pp. 210-211.

[205] Parlamento Europeo, *Relazione sulle implicazioni dei* Big Data *per i diritti fondamentali*, op. cit., Paragrafo 7.

[206] Recepito nell'art. 16, co. 2, D.Lgs. 51/2018.

[207] Recepito nell'art. 23, co. 1, D.Lgs. 51/2018.

prevenzione generale e soccorso pubblico fino a 5 anni dalla raccolta (lett. l)); i dati relativi a controlli di polizia fino a 20 anni dalla raccolta (lett. m)); i dati raccolti per l'analisi criminale e di prevenzione fino a 10 anni dall'elaborazione dell'analisi (lett. n)).

È consentito il trattamento dei dati personali per esigenze temporanee o in relazione a situazioni particolari che sono direttamente correlate all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria (art. 8, co. 1). I dati personali trattati per esigenze temporanee «sono conservati separatamente da quelli registrati permanentemente, per un periodo di tempo non superiore a quello necessario agli scopi specifici per i quali sono stati raccolti e, comunque, non oltre 10 anni dalla cessazione dell'esigenza o della situazione particolare che ne hanno reso necessario il trattamento» (art. 8, co. 3). Inoltre, a scopo di cautela, i nuovi sistemi informativi e programmi informatici devono essere progettati in modo che i dati personali siano cancellati o resi anonimi, con modalità automatizzate, allo scadere dei termini di conservazione previsti e in modo da consentire la documentazione in appositi registri degli accessi e delle operazioni effettuati dagli operatori abilitati (art. 8, co. 4).

Dunque, posto che l'accesso alle informazioni dovrà essere limitato ad un numero ristretto di operatori formati, i dati forniti agli algoritmi di polizia predittiva dovranno essere stati oggetto di anonimizzazione ed assunti nella quantità strettamente necessaria per le finalità di prevenzione. Date queste premesse ed indicazioni, però, occorre fare una differenziazione tra i dati già in possesso delle forze di polizia, quelli raccolti a seguito del fatto criminoso dagli operatori di polizia giudiziaria e, infine, quelli estratti da altre fonti dai dispositivi stessi, viste le differenze qualitative e d'origine. I dati contenuti in denunce ed atti giudiziari danno garanzie in termini di neutralità, affidabilità (provengono dalla PA) e di circoscrizione agli elementi strettamente necessari per la finalità di lotta al crimine, ma dovranno essere oggetto di anonimizzazione. Le informazioni riguardanti nuovi fatti criminosi sono riferite direttamente al fatto (come immagini di telecamere e tracce biologiche) ed estratte da moduli *ad hoc* compilati dai soggetti interessati offesi dal reato assunti – nel contesto italiano, a sommarie informazioni (art. 351, c.p.p.) – ad opera della polizia giudiziaria; sono quindi anonime, affidabili e neutre. I maggiori problemi si pongono, invece, con i dati raccolti dall'algoritmo da altre fonti: infatti, questi dovranno essere oggetto di accurata anonimizzazione, il loro grado di affidabilità e neutralità dipenderà dalla fonte d'origine (ad esempio, banche dati di un fornitore di un servizio, piuttosto che le piattaforme sociali) e dovranno limitarsi a quelli strettamente necessari alla finalità del trattamento.

È opportuno, a questo punto, sottolineare che, affinché i dispositivi di polizia predittiva siano ritenuti compatibili con gli ordinamenti continentali e rispettosi del fine per il quale sono adottati, devono processare dati riferiti a soggetti che effettivamente hanno commesso un crimine;

inoltre, le loro elaborazioni non devono determinare la sensazione che tutte le persone con comportamenti predefiniti preoccupanti o a rischio siano tenute sotto sorveglianza. Il profilo del criminale processato dal sistema deve essere sempre ancorato ai riscontri già avuti sul campo (legati a precedenti denunce, immagini di telecamere, ecc.), quindi riferito ad una persona specifica, per quanto ancóra anonima. La profilazione fatta a priori sulla mera base di statistiche porta inevitabilmente ad effetti discriminatori e ciò si coglie maggiormente con i dispositivi di polizia predittiva che individuano le zone calde: in questo secondo caso, infatti, gli operatori di polizia saranno potenzialmente portati a controllare indiscriminatamente tutta una serie di persone per il solo fatto di appartenere al profilo segnalato. Proprio per evitare tali conseguenze, l'art. 11[208] della Direttiva vieta che le decisioni assunte dalle forze di polizia si fondino «unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato», a meno che non siano previste delle garanzie adeguate, tra cui «almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento» (par. 1). La profilazione che conduce alla «discriminazione di persone fisiche sulla base di categorie particolari di dati personali» è, invece, sempre vietata (par. 3).

Il fatto di per sé, invece, di determinare automaticamente una strategia di pattugliamento non incontra alcun tipo di ostacolo legale da parte dell'art. 11: in effetti, «*les mesures d'organisation du service, telles que l'orientation des patrouilles, ne sont pas des décisions individuelles produisant des effets juridiques*»[209].

L'individuazione a priori di persone sospette collide anche con la presunzione di innocenza[210], di cui all'art. 6, par. 2 CEDU e art. 27 Cost., per il quale «[o]gni persona accusata di un reato è presunta innocente fino a quando la sua colpevolezza non sia stata legalmente accertata». La norma non può, però, essere presa in considerazione per cogliervi dei principi guida, quando si tratti di Polizia Predittiva: infatti, è ancorata alla tradizionale attività reattiva delle forze di polizia e, per questo, «*do[es] not provide satisfactory answers to violations caused to the principle of the presumption of innocence perpetrated by surveillance systems*»[211]. Pensata per un contesto nel quale la legge penale era considerata l'*extrema ratio*, nel moderno sistema nel quale l'ago della bilancia si trova a metà via tra la prevenzione e la repressione come a rappresentare una saldatura tra i due momenti, la presunzione di innocenza va ridefinita.

---

[208] Recepito nell'art. 8, D.Lgs. 51/2018.

[209] Tradotto: «le misure rivolte all'organizzazione di un servizio, come quello della disposizione delle pattuglie, non sono decisioni riguardanti l'individuo che producono effetti giuridici». C. CASTETS-RENARD – P. BESSE – J. LOUBES – L. PERRUSSEL, *Encadrement des risques techniques et juridiques*, op. cit., p. 46.

[210] In argomento, M. MENDOLA, *One Step Further in the "Surveillance Society"*, op. cit., pp. 16-22. Per approfondire sulla presunzione di innocenza, si veda cfr. P.P. PAULESU, *La presunzione di non colpevolezza dell'imputato*, Giappichelli Editore, Torino 2009.

[211] Tradotto: «non offre risposte soddisfacenti in caso di violazione al principio di presunzione di innocenza perpetrato da sistemi di sorveglianza». *Idem*, p. 19.

Se, nel senso tradizionale, la presunzione di innocenza comporta che le autorità competenti possano, nella fase delle indagini, avanzare un sospetto su una persona solo quando è stato commesso un reato – vi è, quindi, un'offesa specifica e concreta da contestare – e vi sono sufficienti elementi oggettivi per provare la sua colpevolezza[212] e che, durante il procedimento, siano tenute a rispettare una serie di garanzie riconosciute all'indagato-imputato, tale impostazione non è sufficiente a porre dei limiti durante la fase preventiva e va arricchita di accorgimenti.

Utilizzando sistemi statistici e la profilazione, come già indicato, è, infatti, concreto il rischio che tutte le persone siano trasformate in potenziali sospetti e ciò ha inevitabili ricadute sul principio della presunzione di innocenza. Per porre dei correttivi a tale conseguenza, è dunque necessario che le informazioni processate dai dispositivi di polizia predittiva: non siano in alcun caso ritenute da sole sufficienti per avallare il sussistere di un ragionevole sospetto; siano riferite ad uno specifico profilo di persona ricercata e contengano quante più dettagli possibili per permettere agli operatori di polizia di effettuare un controllo mirato; siano frutto di dati aggiornati.

La presenza di tali garanzie metodologiche anche in questa fase potrebbe, a fronte di un principio che diventa più labile, divenire *a contrario* un'ulteriore tutela per i cittadini perché l'intervento delle forze di polizia sarebbe stato determinato da un'ulteriore attività di valutazione *ex ante* sull'idoneità degli elementi a carico a giustificare la misura effettuata o richiesta (non ci sarebbe quindi la sola valutazione *ex post* del magistrato).

In sostanza, gli operatori di polizia devono decidere cosa fare con i risultati dell'elaborazione dei dispositivi, confrontandoli con altre informazioni in loro possesso, e non devono mai appiattirsi sugli stessi. In questo modo, l'algoritmo di polizia predittiva rimane uno strumento a servizio delle attività di polizia amministrativa e di sicurezza e non si pone come il solo in grado di stabilirne a monte l'espletamento, con tutta la serie di potenziali violazioni ai diritti fondamentali che ne seguirebbero.

Altro quesito che è stato sollevato riguarda la possibilità di utilizzare i risultati prodotti in sede di accertamento investigativo per attribuire ad un soggetto altri reati consumati in precedenza. Se nessun dubbio si riscontra circa le modalità di raccolta dei dati, che dovranno essere stati acquisiti – sia per le forme sia per i termini temporali – in ossequio alle indicazioni codicistiche[213], le incertezze si pongono in merito ai risultati delle correlazioni processate dall'algoritmo

[212] Cfr. Corte EDU, sentenza Guzzardi c. Italia (ricorso n. 7367/76), 6 novembre 1980; Corte EDU, *S. and Marper v. the United Kingdom* (ric. nn. 30562/04 e 30566/04), 4 dicembre 2008 (sentenza reperibile *online* al collegamento https://rm.coe.int/168067d216, consultato da ultimo in data 21 giugno 2022).

[213] Nel contesto italiano, dall'ottica della polizia giudiziaria, solo i diversi elementi storici acquisiti nel rispetto della disciplina codicistica potranno essere portati all'attenzione del GIP, in fase di indagine, o del Tribunale, ad esempio, per richiedere una misura cautela, o formati in dibattimento, senza incorrere in un formale divieto di utilizzabilità (art. 191, c.p.p.).

nell'individuare il collegamento criminale tra i diversi fatti di reato[214]. In questo caso, nascono delle frizioni, oltre che con la presunzione di innocenza, con il diritto di difesa, di cui all'art. 48, Carta di Nizza. Infatti, «*le manque de transparence et connaissance des outils de police prédictive est susceptible de porter atteinte aux droits de la défense, si la partie désignée par le système comme étant potentiellement dangereuse ne connaît ni les données utilisées ni le fonctionnement de l'outil, ce qui l'empêche de remettre en cause la pertinence des résultats obtenus et donc d'exercer pleinement ses droits de la défense. Le principe de transparence algorithmique est indispensable non seulement pour le traitement des données personnelles mais aussi pour l'exercice des droits de la défense en justice*»[215]. In questa situazione, le modalità di utilizzo del dispositivo dovranno necessariamente essere caratterizzate da trasparenza ed esplicabilità[216], in quanto il soggetto destinatario della misura di polizia, nel rispetto del diritto di difesa, dovrebbe poter impugnare la decisione per verificarne, in contraddittorio, presupposti, opportunità e legalità (v. *infra*).

2.2.3 Precauzioni e linee orientative in tema di polizia predittiva.

Come visto, l'utilizzo degli strumenti di polizia predittiva non è disciplinato da normative di settore ed è lasciato alla sensibilità ed alla valutazione dei progettisti, prima, e degli operatori di polizia, poi; non a caso, la CEPEJ fa ricadere questi dispositivi informatici nella serie di strumentazioni che potrebbero essere compatibili con i principi gli ordinamenti giuridici europei, a patto che si adottino «notevoli precauzioni metodologiche»[217] nel loro sviluppo per evitare siano violati i diritti fondamentali e si generino effetti distorsivi, come, per esempio, «un forte "effetto performativo" (in un dato luogo vi è maggiore possibilità di scoprire un reato e ciò rafforza poi il sistema)»[218].

La prima precauzione da considerare riguarda il tipo di strumentazione da adottare: chi scrive ritiene che i dispositivi di polizia predittiva compatibili con i sistemi occidentali e con l'ordinamento giuridico italiano siano quelli che analizzano le condotte seriali e cicliche, ricercando

[214] Diverso è, invece, il tema della possibilità di utilizzare i risultati delle correlazioni elaborate come mero spunto investigativo, destinato ad essere integrato da altre autonome fonti di prova.

[215] Tradotto: «la mancanza di trasparenza e di conoscenza degli strumenti di polizia predittiva è idonea a ledere i diritti della difesa, se il soggetto designato dal sistema come potenzialmente pericoloso non conosce né i dati utilizzati, né il funzionamento dello strumento, il che gli impedisce di mettere in discussione la rilevanza dei risultati ottenuti e dunque esercitare pienamente i propri diritti di difesa. Il principio della trasparenza algoritmica è essenziale non solamente per il trattamento dei dati personali, ma anche per l'esercizio dei diritti di difesa in giudizio». C. CASTETS-RENARD – P. BESSE – J. LOUBES – L. PERRUSSEL, *Encadrement des risques techniques et juridiques*, op. cit., p. 40.

[216] In tema di trasparenza dell'algoritmo, l'azienda produttrice di PredPol, per esempio, ha indicato nel suo sito Internet l'algoritmo utilizzato dal suo applicativo per elaborare i dati (reperibile *online* al collegamento https://www.predpol.com/technology/, consultato da ultimo in data 21 giugno 2022). La scelta è stata anche indotta dal fatto che, avendo brevettato l'algoritmo, i suoi elementi sono stati comunque resi di pubblico dominio.

[217] Così, CEPEJ, *Carta etica europea*, *Appendice II*, cit., p. 43.

[218] *Idem,* p. 43.

il collegamento criminale. Tali programmi «nulla p[ossono] per prevenire o accertare fatti criminali occasionali o fatti anche potenzialmente seriali all'atto della loro insorgenza, ma [si prestano a dare ottimi risultati] per quelle forme di reiterazione delittuosa che integrano – tra l'altro – l'impatto criminale socialmente (e penalmente) più grave e quindi meno "accettabile"»[219]. Questi ultimi, rispetto a quelli che individuano le zone calde, hanno anche il vantaggio di evitare agli operatori di polizia di mettere in atto azioni di controllo causale ed indiscriminato delle persone, in quanto saranno sorvegliate solo quelle corrispondenti al profilo segnalato; se l'azione di appostamento non si traduce in un'attività di deterrenza, gli operatori potranno comunque intervenire immediatamente prima o durante l'atto criminale. Le tecniche di individuazione delle zone calde, tra l'altro, presentano forti profili di incompatibilità con il principio della presunzione di innocenza, a causa del loro intrinseco funzionamento.

Altra precauzione consiste nella scelta e nel trattamento dei dati: oltre al rispetto di quanto previsto dalla Direttiva (UE) n. 2016/680, il programma dovrà poter elaborare dati anonimi, sicuri, completi ed aggiornati.

Gli operatori di polizia devono comunque sempre avere l'ultima parola sul da farsi, così da sottolineare il mero ruolo ancillare di questi dispositivi rispetto alla volontà umana e, così, anche scongiurare una «possibile "tirannia dell'algoritmo" che potrebbe minimizzare o addirittura sostituire progressivamente il giudizio umano»[220].

Nell'ambito italiano, il Ministero dell'Interno – Dipartimento della Pubblica Sicurezza sarebbe opportuno che sviluppasse un proprio strumento di polizia predittiva, per evitare che la materia pubblicistica della sicurezza sia lasciata in mano alla logica commerciale delle aziende private. In tale maniera, sarebbe anche più semplice rispondere alle esigenze di trasparenza ed esplicabilità dell'algoritmo. Al momento, gli algoritmi KeyCrime ed XLAW sono sì di proprietà di aziende private, ma sono stati sviluppati e sono continuamente aggiornati da ex agenti di Polizia, che, per formazione e sensibilità, hanno ben chiari i principi ed i limiti ordinamentali in cui opera la polizia di sicurezza. La situazione attuale può essere considerata come un compromesso accettabile, ma che deve essere a termine: in senso provocatorio, c'è da chiedersi se i prodotti saranno ancóra in linea con tutti i vincoli legali e morali di settore, quando in futuro agli attuali proprietari subentreranno altre figure senza un passato nelle forze di polizia, quindi senza la loro conoscenza e sensibilità.

Il Ministero dell'Interno deve incoraggiare la cooperazione con le università ed i gruppi scientifici per sviluppare ed implementare un *software* di proprietà pubblica; inoltre, il fatto che il dispositivo sia elaborato in contesto accademico ne favorirebbe l'accettabilità da parte della società,

[219] In questi termini, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 56.
[220] Così, CEPEJ, *Carta etica europea*, *Appendice II*, cit., p. 35.

più che altro in merito alle tematiche di trasparenza e di esplicabilità.

Infine, forse nel tentativo di mitigare il fenomeno – descritto in introduzione – di maggiore autonomia delle forze di polizia dalla magistratura requirente, la CEPEJ non manca di sottolineare come «[l]'analisi penale mediante approcci che combinano sistemi di informazione geografica (GIS) e notevoli quantità di dati dei procedimenti potrebbe essere condivisa in modo migliore con i pubblici ministeri»[221]. Infatti, in un sistema sempre più improntato sulla proattività in cui si fa più incerto il momento del passaggio dalla funzione di polizia amministrativa a quella di polizia giudiziaria, la possibilità di coinvolgere la magistratura inquirente anche nel tema del mantenimento dell'ordine pubblico potrebbe fare da correttivo e creare un maggiore coordinamento tra tutte le forze chiamate ad occuparsi della sicurezza dal momento preventivo al momento repressivo. Nel sistema nazionale, questo si potrebbe tradurre in una partecipazione più stabile – e non saltuaria – dei componenti dell'ordine giudiziario al Comitato Provinciale per l'Ordine e la Sicurezza Pubblica, organo consultivo di cui si avvale il Prefetto quale responsabile provinciale dell'ordine e della sicurezza pubblica[222]. Il Comitato potrebbe essere la sede nella quale le Istituzioni solitamente impegnate nella pubblica sicurezza e la magistratura inquirente – nel rigoroso rispetto delle rispettive competenze – potrebbero organizzare una risposta più efficiente al crimine e rinsaldare il sistema, per come tradizionalmente strutturato: le prime potrebbero informare la seconda sulle attività di controllo preventive in essere, permettendole di riassumere, in un certo senso, il ruolo centrale attribuitole dalla Costituzione nella risposta repressiva (in una lettura meno rigida dell'art. 112, nella quale il pubblico ministero può attendere di esercitare l'azione penale, se ciò serve a rintracciare altri criminali e smantellare strutture complesse dedite alla delinquenza); invece, la seconda potrebbe indicare alle prime accorgimenti di metodo e problematiche legali in ordine alla raccolta di informazioni – potenziali prove a carico da portare all'attenzione del GIP o del Tribunale – e porre così le basi per un'azione nel complesso più incisiva e rispettosa dei diritti, che non trovano nella fase preventiva una trattazione altrettanto puntuale a quella prevista nel momento procedimentale.

[221] *Idem*, p. 43. Analogamente, sempre la CEPEJ, *Idem*, p. 43, ribadisce il concetto, affermando che «questo tipo di applicazione potrebbe riguardare non soltanto la polizia ma anche i pubblici ministeri negli organi di prevenzione dei reati di cui fanno parte».

[222] Cfr. art. 20, L. 121/181. Presieduto dal Prefetto, il Comitato Provinciale per l'Ordine e la Sicurezza Pubblica è di base composto dal Questore, dal Comandante Provinciale dei Carabinieri e dal Comandante il Gruppo Guardia di Finanza (oltre che dal sindaco del comune capoluogo e dal presidente della provincia), ma tale composizione è allargabile a soggetti esterni all'amministrazione della pubblica sicurezza (co. 3). Al momento, il Prefetto, ai sensi del co. 4, «può» invitare alle riunioni anche componenti dell'ordine giudiziario. La partecipazione dei pubblici ministeri a quel tavolo non è quindi sistemica, ma è rimessa alla discrezionalità ed alla sensibilità del singolo Prefetto.

2.3 *Big data analytics* come «baionette» contro la corruzione.[223]

Come visto, la digitalizzazione e l'implementazione di piattaforme per interoperabilità dei dati delle pubbliche amministrazioni favoriscono la trasparenza e sono alla base dell'adozione di sistemi di *big data analytics*, cioè di dispositivi di IA capaci di operare in attività di monitoraggio e gestione del rischio corruzione (rientranti tra le misure anticorruzione in senso stretto). Se per il contesto pubblico italiano non si ha notizia di sperimentazioni in atto e si è in piena attività di digitalizzazione della PA, anche in quei Paesi[224] che stanno sperimentando progetti più o meno pionieristici «*using AI technologies to curb corruption is still in its early phase of implementation*»[225].

Al contrario, è nel settore privato, specie nel sistema anglosassone, che alcune realtà imprenditoriali, con atteggiamento proattivo e svincolato dall'indicazione di specifici obblighi normativi, hanno già fatto affidamento su sistemi di *big data analytics* per prevenire fenomeni corruttivi al loro interno che possano danneggiare le aziende stesse. Anche in questo caso, quindi, gli enti privati hanno anticipano nella prassi il legislatore e sono diventati per il settore pubblico fonte di ispirazione da cui, *mutatis mutandis*, trarre idee e soluzioni per elaborare strategie e introdurre strumenti a fini di anticorruzione: non a caso, lo stesso PTPCT era stato pensato prendendo spunto dal modello 231, l'atto di autoregolamentazione con il quale gli amministratori dell'azienda, individuati specifici reati da prevenire e formato adeguatamente il personale, mirano ad evitare che i comportamenti scorretti dei dipendenti possano determinare anche sanzioni per l'impresa (artt. 6 e 7 D.Lgs. 231/2001).

Gli enti collettivi hanno fatto affidamento su strumenti informatici automatizzati di raccolta, elaborazione e analisi di grandi quantità di dati interni ed esterni all'impresa per raggiungere tre obiettivi: «1) identificare indicatori di anomalia e rischio corruzione, nonché ulteriori segnali d'allarme nelle operazioni aziendali (in particolare azioni anomale rispetto ai modelli di comportamento che il sistema qualifica come ricorrenti/ordinari); 2) monitorare il traffico *mail* interno, allo scopo di individuare conversazioni in cui si utilizzino determinate parole chiave

---

[223] «Ci sono due modi per governare gli italiani: con le baionette o con la corruzione» (Vittorio Emanuele II, rivolgendosi al plenipotenziario inglese August Paget, 6 luglio 1867).

[224] Oltre alle esperienze cinese ed ucraina già citate, per una breve descrizione di una serie di iniziative già intraprese in alcuni Paesi, si veda P. AARVIKPP (a cura di), *Artificial Intelligence – a promising anti-corruption tool in development settings?*, in www.u4.no, Report n. 1/2019, U4 Anti-Corruption Resource Centre, Bergen 2019, pp. 4 e ss. (reperibile *online* al collegamento https://beta.u4.no/publications/artificial-intelligence-a-promising-anti-corruption-tool-in-development-settings.pdf, consultato da ultimo in data 21 giugno 2022); S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., p. 65 (si riferisce ai dispositivi statunitensi MENTAS e NORCOM). Per gli esperimenti nello specifico contesto brasiliano, F. ODILLA, *Bots against corruption: Exploring benefits and limitations of AI-based anti-corruption technology*, Digital Media, Machine Learning, and Corruption: How the Newest Technological Development Facilitate and Curb Corruption Practices Across the World, 2021.

[225] Tradotto: «l'utilizzo di tecnologie di IA per ostacolare la corruzione è ancóra nella prima fase di realizzazione». N. KÖBIS – C. STARKE – I. RAHWAN, *Artificial Intelligence as an Anti-Corruption Tool*, op. cit., p. 18.

considerate "a rischio"; 3) fornire al *management* un *report* in *real-time* in merito a eventuali profili di anomalia (o altri *red flags*) nel comportamento del (o nei dati raccolti sul) *partner*/agente con cui sono in corso determinate operazioni (c.d. *third party due diligence*)»[226].

Tra gli elementi oggetto di segnalazione in caso di anomalia vi sono, ad esempio, prezzi d'acquisto, compensi per consulenze e flussi di denaro anomali rispetto alla media dei prezzi di riferimento del settore commerciale e dell'area geografica, possibili conflitti di interesse tra terze parti e dipendenti coinvolti nelle operazioni e compensi[227].

Ora, ipotizzando che nell'ambito pubblico si diffondano dispositivi di IA per finalità di anticorruzione, questi si rivelerebbero più efficaci in un'ottica di prevenzione *lato sensu* o di prevenzione mirata? In altre parole, potrebbe essere più fruttuoso adottare un algoritmo in grado di prevedere la corruzione, sulla scorta di quanto fanno i dispositivi di polizia predittiva sopra analizzati, oppure "solamente" capace, attraverso la segnalazione di profili di anomalia, di scovare un reato di corruzione o una situazione di mala amministrazione già in atto? A parere di chi scrive, potrebbero essere valide entrambe le opzioni, ma con una decisa propensione verso la seconda, per una serie di motivi.

In primo luogo, c'è da considerare la struttura del reato che si intende prevenire: infatti, il fenomeno corruttivo si caratterizza per il fatto di portare sia il pubblico ufficiale che il privato ad ottenere un guadagno dal *pactum sceleris*, attraverso il quale il primo accetta dal secondo, per un atto relativo alle proprie attribuzioni e favorevole verso quest'ultimo, un compenso che non gli è dovuto. Di conseguenza, non vi è, come nei reati predatori, una persona offesa che denuncia alle autorità l'accaduto. Dunque, «[l]a corruzione è, per sua natura, un'attività sommersa»[228]: nessuna delle parti ha interesse a rendere noto il fatto e a lasciare traccia delle attività e ciò si traduce in una mancanza di dati da sottoporre ad un *software* per un'elaborazione predittiva legata alla serialità. Sul punto, basti ricordare come il *Corruption Perception Index*, l'indice di maggior celebrità utilizzato da Transparency International nello stilare la classifica dei Paesi in cui il fenomeno corruttivo è più o meno avvertito, si basi appunto anche sui livelli di corruzione percepita e non solo su quelli accertati[229]. Anche se la limitata quantità di dati permetterebbe ugualmente di fare delle

[226] Così, E. BIRRITTERI, Big Data Analytics *e* compliance *anticorruzione*, op. cit., p. 290.

[227] Cfr. *Idem*, p. 291. Per una breve panoramica di questi indicatori, si veda D. BERLINER – K. DUPUY, *The promise and perils of data for anti-corruption efforts in international development work*, U4 Brief, n. 7/2018, U4 Anti-Corruption Resource Centre, Bergen 2018 (reperibile *online* al collegamento https://www.u4.no/publications/the-promise-and-perils-of-data-for-anti-corruption-efforts-in-international-development-work, consultato da ultimo in data 21 giugno 2022).

[228] In questi termini, M. GNALDI, *Indicatori di corruzione e nuovi indicatori di prevenzione della corruzione*, in M. GNALDI – B. PONTI (a cura di), *Misurare la corruzione oggi*, Franco Angeli, Milano 2018, p. 34.

[229] In merito, si veda https://www.transparency.it/indice-percezione-corruzione, consultato da ultimo in data 21 giugno 2022. Inoltre, sulla scarsità di dati, cfr. ANAC, *La corruzione in Italia (2016-2019*), op. cit., p. 2: tra il 2016 e il 2019 in Italia sono state spiccate dall'Autorità giudiziaria 117 custodie cautelari e, analizzando i provvedimenti della magistratura, si segnalano 152 casi di corruzione «(solo a considerare quelli scoperti)».

previsioni, queste sarebbero legate alla semplice presenza in una zona di alcuni parametri (ritenuti sintomatici) o all'appartenenza ad un determinato ufficio e non all'effettivo comportamento anomalo o infedele di un dipendente pubblico. Si riprodurre quindi il rischio di discriminazione proprio degli strumenti di polizia predittiva tarati sul modello *hotspot*.

Anche ammettendo che un dispositivo con tali modalità di funzionamento venisse utilizzato, ciò porterebbe semplicemente a maggiori controlli sugli atti compiuti dai dipendenti incardinati in uffici in cui si svolgono passaggi amministrativi cruciali per il risultato finale del procedimento: nulla di nuovo, in Italia, rispetto a quanto già stabilito dalle linee guida sui PTPCT, che obbligano le amministrazioni stesse a procedimentalizzare il rischio corruzione – quindi, ad effettuare maggiori controlli e prevedere misure di prevenzione *ad hoc* – secondo le caratteristiche specifiche e il grado di rischio di ogni singolo ufficio.

Pertanto, un *software* predittivo anticorruzione indicherebbe solo, in modo generale, quali zone del Paese o quali uffici aventi lì la sede potrebbero essere più facilmente permeabili ai fenomeni corruttivi. Al contrario, un algoritmo che indicasse profili di anomalia, oltre ad avere un effetto dissuasivo diretto, identificherebbe esattamente quale dipendente dovrebbe essere oggetto di controllo, evitando approcci generici e discriminatori basati su zone di lavoro e/o tipo di ufficio.

La predizione generale della corruzione per mezzo di algoritmo è, invece, il modello su cui ha puntato uno studio realizzato dall'Università di Valladolid[230]. I ricercatori ritengono di aver dimostrato che è possibile predire in anticipo casi di corruzione attraverso l'analisi delle circostanze che favoriscono il sorgere del fenomeno. Inoltre, «*[u]nlike previous research, which is based on the perception of corruption, […] data on actual cases of corruption [is used]*»[231]: infatti, la previsione è realizzata a partire dai dati contenuti nell'archivio del quotidiano *El Mundo*, che raccoglie fattori macroeconomici e politici e fa riferimento a vicende verificatesi in Spagna tra il 2000 e il 2012, riportate dalla stampa o che hanno avuto delle conseguenze a livello giudiziario[232]. Nello specifico, il sistema di intelligenza artificiale implementato è in grado di individuare le province spagnole che corrono maggiori rischi di corruzione sulla base di variabili economiche e politiche che, secondo gli studi di settore, favoriscono il sorgere della corruzione: tra questi, la tassazione immobiliare e l'aumento dei prezzi degli immobili, la crescita economica, il numero di istituti di deposito presenti, l'indice di disoccupazione e il permanere al potere dello stesso partito politico per lunghi periodi di

[230] F.J. LÓPEZ-ITURRIAGA – I. PASTOR SANZ, *Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces*, in *Social Indicators Research: An International and Interdisciplinary Journal for Quality-of-Life Measurement,* vol. 140**,** n. 3/2018, pp. 975-998 (pubblicato *online* il 27 novembre 2017 e ivi reperibile dal collegamento https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075828, consultato da ultimo in data 21 giugno 2022).

[231] Tradotto: «a differenza delle precedenti ricerche, che si basavano sulla percezione della corruzione, sono usati dati riferiti a casi reali». *Idem*, p. 2.

[232] Cfr. *Idem*, p. 13.

tempo[233].

A seconda delle caratteristiche di ciascuna provincia analizzata, sarebbe possibile stimare la probabilità di casi di corruzione emergenti in un periodo di tre anni. Mentre in alcune circostanze i casi di corruzione possono essere previsti prima che si verifichino e ciò consente l'attuazione di misure preventive, in altri casi il periodo di previsione è molto breve, rendendo quindi necessario adottare urgentemente misure correttive. In sostanza, questo sistema di intelligenza artificiale permetterebbe alle autorità di identificare le vulnerabilità e indirizzare i controlli in particolari aree a rischio o su operazioni sospette e/o da monitorare nel tempo.

Tuttavia, gli stessi ricercatori avvertono la necessità di porre dei correttivi ai risultati ottenuti dall'elaborazione del loro *software*: infatti, questi non significano «*that economic growth or a given party remaining in power causes public corruption but that the fastest growing regions or the ones ruled by the same party for a long time are the most likely to be involved in corruption cases. Economic growth* per se *is not a sign of corruption, but rather it increases the interactions between economic agents and public officers. Similarly, being in office too long might prove to be an incentive for creating a network of unfair relations between politicians and economic agents. In addition, more competitive markets may induce some agents to pay bribes in order to obtain public concessions or a better competitive position*»[234]. Se da un lato non si mettono in discussione la correlazione trovata tra certi indici ed i fenomeni corruttivi e le osservazioni sistematiche fatte dai ricercatori, dall'altro, indirettamente, si mostrano i limiti legati a questo tipo di *software*: infatti, le predizioni sono generiche e non legate a concreti ed anomali comportamenti adottati da funzionari pubblici (che, si badi bene, possono essere sempre *ex post* giustificabili in relazione allo specifico procedimento a cui si riferiscono).

Nell'opinione di chi scrive, un'impostazione predittiva *lato sensu* non produrrebbe una maggior scoperta di fatti di corruzione, in quanto le risorse umane deputate al controllo sarebbero semplicemente destinate in contesti ritenuti ad alto rischio senza che vi siano elementi oggettivi a carico di qualche dipendente pubblico: di fatto, la predizione non farebbe altro che confermare quanto già si sa, e cioè che certi uffici, impegnati in fasi sensibili del procedimento, sono più esposti al rischio di corruzione di altri. Diversamente, un dispositivo che – a prescindere dall'ambiente in cui opera il dipendente – si limitasse a segnalare profili di anomalia effettivamente riscontrati

[233] Cfr. *Idem*, pp. 14 e ss.

[234] Tradotto: «che la crescita economica o il fatto che un dato partito rimanga al potere causi la corruzione pubblica, ma che le regioni che crescono più velocemente dal punto di vista economico o che sono amministrate dallo stesso partito per un lungo periodo sono quelle che più facilmente saranno coinvolte in casi di corruzione. La crescita economica *per se* non è un segno di corruzione, ma piuttosto aumenta le interazioni tra gli operatori economici e i pubblici ufficiali. Allo stesso modo, stare in carica troppo a lungo potrebbe rivelarsi un incentivo per creare una rete di relazioni sleali tra i politici e gli agenti economici. Inoltre, mercati più competitivi potrebbero indurre alcuni operatori a pagare tangenti con l'obiettivo di ottenere concessioni pubbliche o una migliore posizione concorrenziale». *Idem*, pp. 30-31.

rispetto a modelli procedimentali ideali potrebbe indirizzare le attività di controllo su circostanziate ed incontrovertibili operazioni sospette, aumentando così le probabilità che siano scoperti fenomeni corruttivi già in atto o situazioni di mala amministrazione. Per esempio, calandoci nello specifico contesto degli appalti pubblici, gli indicatori di rischio potrebbero segnalare bandi di gara con termini stranamente brevi per la presentazione delle offerte, prezzi d'acquisto ingiustificati o un andamento delle offerte anormale che possa nascondere l'esistenza di un cartello commerciale tra le imprese interessate e tutelato dal pubblico ufficiale infedele[235]. In Italia, l'Autorità nazionale anticorruzione, consapevole di come «l'elaborazione di opportuni indicatori statistici di sintesi (*red flags*) sia suscettibile di indirizzare l'attività di vigilanza in modo mirato verso le situazioni potenzialmente di maggiore criticità»[236], già da tempo è impegnata nella definizione di metodologie volte alla loro costruzione e, in tal senso, ha pubblicato nel 2018 lo studio *Efficienza dei contratti pubblici e sviluppo di indicatori di rischio corruttivo*[237].

Tra l'altro, il fatto che gli studiosi non indichino in che modo le autorità, seguendo la predizione, potrebbero migliorare «*the efficiency of the measures aimed at fighting corruption*»[238], conferma nuovamente l'incapacità di questo tipo di dispositivo di indicare esattamente quale operazione mettere sotto controllo: non conoscendo il problema, non si può nemmeno valutare quale strumento utilizzare per risolverlo. Tra l'altro, nel contesto italiano, per motivi sistematici un dispositivo così impostato non darebbe un *quid pluris* nelle attività di prevenzione: infatti, nel PTPCT (e, oggi, nel nuovo PIAO di cui all'art. 6 D.L. 80/2021) l'adozione di particolari misure per abbassare il rischio di corruzione è necessariamente demandata alle dirette amministrazioni e legata alle specifiche caratteristiche dell'ente e dei singoli uffici (non sono le autorità che devono adottare, di volta in volta, misure straordinarie per fronteggiare il rischio corruzione).

Infine, un'ultima considerazione sui dati utilizzati dal dispositivo spagnolo permette di ribadire il problema relativo alla quantità e all'attendibilità dei dati posti al centro dell'analisi informatica. Come già visto parlando dei dispositivi di polizia predittiva, i dati elaborati devono provenire da fonti affidabili e sicure per fare in modo che i fattori di rischio e anomalia individuati possano essere ritenuti attendibili. Nel caso del *software* spagnolo, i dati sono estratti dalla banca dati del quotidiano *El Mundo*: mentre quelli tratti dai provvedimenti giudiziari sono sicuramente

---

[235] Cfr. M. FAZEKAS – E. DÁVID-BARRETT, *Corruption Risks in UK Public Procurement and New Anti-Corruption Tools,* Government Transparency Institute, Budapest 2015, p. 28 (reperibile *online* al collegamento http://www.govtransparency.eu/wp-content/uploads/2016/10/Fazekas-David-Barrett_Public-procurement-review_public_151113.pdf, consultato da ultimo in data 21 giugno 2022).

[236] ANAC, G. MARINO – F. SBICCA (a cura di), *Efficienza dei contratti pubblici e sviluppo di indicatori di rischio corruttivo*, 2018, p. 3 (reperibile *online* al collegamento https://www.anticorruzione.it/documents/91439/54fcab35-54b0-35d7-88fa-5ace3249fbcf, consultato da ultimo in data 21 giugno 2022).

[237] *Idem*.

[238] Tradotto: «l'efficienza delle misure tese a combattere la corruzione». F.J. LÓPEZ-ITURRIAGA – I. PASTOR SANZ, *Predicting Public Corruption*, op. cit., p. 31.

sicuri[239], altrettanto non può dirsi per quelli ricavati dagli articoli di stampa o presenti in Internet.

In generale, l'aspetto della qualità dei dati da utilizzare solleva maggiori criticità per l'ambito privato. Le pubbliche amministrazioni, infatti, possiedono «un patrimonio informativo composto da atti pubblici di varia natura e di intrinseca affidabilità (stante, appunto, la loro natura pubblicistica), nonché diverse banche dati – come, ad esempio, quella degli appalti pubblici – i cui contenuti si rivelano preziosi per individuare possibili *red flag* di interesse per la prevenzione della corruzione»[240]. Per quanto riguarda l'Italia, una volta conclusa la fase di realizzazione della Piattaforma Nazionale Digitale Dati di cui all'art. 50-*ter* CAD, che risolverebbe l'annoso problema di stabilire l'interoperabilità tra le diverse banche dati pubbliche, i *big data analytics* offrirebbero una soluzione significativa all'incapacità di incrociare dati eterogenei e trarne utili informazioni[241] per finalità di anticorruzione.

Passo successivo sarebbe quello di addestrare gli algoritmi sulla base di metodologie di analisi informatica complete, spiegabili e ispirate alle pratiche empiriche di individuazione e gestione del rischio di corruzione. Per raggiungere tale obiettivo, i tecnici dei Ministeri potrebbero implementare gli algoritmi prendendo come riferimento gli accorgimenti e le misure standardizzate, procedimentalizzate o personalizzate che sono rinvenibili nei PTPCT-PIAO o ispirandosi ai programmi di conformità anticorruzione già adottati da alcune realtà private. In alternativa, l'ANAC potrebbe stilare in collaborazione con AgID delle linee guida e delle regole tecniche base che la PA dovrebbe seguire nella predisposizione dei propri algoritmi di analisi.

In pratica, è auspicabile l'adozione di una regolamentazione pubblicistica sull'utilizzo di queste procedure, visto che, oggi, ogni singolo ente pubblico e privato[242] può decidere quali istruzioni dare, quali analisi far svolgere al sistema e quali dati far elaborare alla macchina.

A queste condizioni, le pubbliche amministrazioni dovrebbero essere in una prima fase incentivate e poi obbligate ad utilizzare questi strumenti, a maggior ragione ora che le *Linee guida per la compilazione del PIAO* invitano espressamente a predisporre e favorire «misure di digitalizzazione», quindi, in senso ampio, ad adottare anche l'intelligenza artificiale, per trattare il rischio corruzione. Considerazioni sul tipo di dati da utilizzare e sul tipo di analisi da effettuare non dovranno però essere lasciate alla mera discrezionalità delle diverse amministrazioni, quantomeno

[239] Sull'utilizzo delle misure giudiziarie come indicatore per misurare la corruzione, cfr. M. GNALDI, *Indicatori di corruzione*, op. cit., pp. 38-39. Se non si pongono particolari problemi dal punto di vista statistico, l'Autrice non manca di sottolineare come «le misure giudiziarie […] present[i]no limiti legati […] alla loro scarsa utilità a fini di prevenzione».

[240] Così, E. BIRRITTERI, Big Data Analytics *e* compliance *anticorruzione*, op. cit., p. 292.

[241] Cfr. M. FALCONE, *La* big data analytics *per conoscere, misurare e prevenire la corruzione*, in M. GNALDI – B. PONTI (a cura di), *Misurare la corruzione oggi*, Franco Angeli, Milano 2018, p. 105.

[242] Dalla prassi sembra emergere come siano le singole società a decidere come strutturare il software di analisi, quali dati inserire nel sistema, quali indagini far svolgere alla macchina, in quali (e in quale segmento temporale delle) procedure aziendali prevederne l'applicazione. Cfr. Consiglio d'Europa, DGI (2017)12. – Committee of experts on Internet Intermediaries (MSI-NET), *Algorithms and Human Rights*, op. cit., p. 6.

per la fase successiva a quella di sperimentazione in qualche amministrazione-pilota, ma andranno regolamentate col tempo. Sarà la politica a dover stabilire l'obbligo di adozione, comuni di utilizzo ed eventuali deroghe. Come già per il PTPCT e il PIAO, che conoscono eccezioni o semplificazioni alla loro applicazione[243], l'adozione cogente di tali algoritmi anticorruzione dovrebbe essere modulata, per andare così incontro alle realtà medio-piccole, che già oggi faticano a rispettare appieno le misure tradizionali previste dalla normativa anticorruzione[244].

A ben vedere, nel generale scivolamento a fini preventivi del diritto penale nel diritto amministrativo, si riscontra anche la tendenza ad allargare il perimetro della prevenzione amministrativa della corruzione: infatti, i controlli non si limitano più soltanto a scoprire comportamenti di eventuale rilevanza penale, ma sono rivolti a ricercare situazioni di mala amministrazione. Dunque, come è stato osservato, «l'identificazione in via informatica di scostamenti dai prezzi standard di settore, eccessi di spesa, anomalie nelle caratteristiche degli appalti e altri *red flags* può diventare un formidabile strumento per eliminare sprechi e combattere inefficienze anche non necessariamente legati a condotte illecite»[245].

Ora, ci si deve domandare come l'ammissibilità di tali procedure possa trovare un bilanciamento rispetto alla disciplina del controllo sui lavoratori e alla tutela della *privacy* e del domicilio informatico del dipendente sottoposto ad accertamento: infatti, per identificare il rischio corruzione in termini di anomalie statistiche e gestionali, i dispositivi di IA, di fatto, attuano una pratica di sorveglianza generalizzata, che, in quanto tale, deve rispettare la normativa e gli orientamenti giurisprudenziali già esistenti in tema.

In generale, tanto nel pubblico che nel privato[246], l'attività dei lavoratori può essere sottoposta a sorveglianza attraverso «impianti audiovisivi e […] *altri strumenti dai quali derivi anche la possibilità di controllo a distanza*»[247] per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale (art. 4, co. 1 L. 300/1970). La possibilità del controllo è subordinata alla sussistenza di un accordo sindacale o, in mancanza,

---

[243] Come già visto, ai sensi dell'art. 6, co. 1 D.L. 80/2021, il PIAO non va adottato dalle pubbliche amministrazioni con meno di cinquanta dipendenti, delle scuole di ogni ordine e grado e dalle istituzioni educative. Queste, si presume, continueranno ad adottare il PTPCT. La stessa adozione del Piano triennale *ex* art. 1, co. 2-*bis* L. 190/2012 non era prevista per società in partecipazione pubblica, associazioni, fondazioni, ecc., ma ANAC – con la delibera n. 8/2015 e con il Piano Nazionale Anticorruzione del 2016 – impose per loro l'obbligo di adottare il modello 231 o modelli di legalità.

[244] In tal senso, l'aggiornamento del 2018 al Piano Nazionale Anticorruzione del 2016 aveva previsto delle misure *ad hoc* nella parte speciale intitolata "*Semplificazioni per Piccoli Comuni*"; pp. 141 e ss. (reperibile *online* al collegamento https://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/Atti/Delibere/2018/PNA_2018.pdf, consultato da ultimo in data 21 giugno 2022).

[245] Così, E. BIRRITTERI, Big Data Analytics *e* compliance *anticorruzione*, op. cit., p. 293.

[246] Ai sensi dell'art. 51, co. 2 D.Lgs. 165/2001 (Testo unico sul pubblico impiego), lo Statuto dei lavoratori si applica anche alle pubbliche amministrazioni.

[247] Corsivo mio.

all'autorizzazione della sede territoriale dell'Ispettorato del lavoro. Inoltre, il terzo comma cristallizza il principio per il quale le informazioni così raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro (si pensi ai procedimenti disciplinari ed alle eventuali sanzioni), «a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli» e sia rispettata la disciplina sulla *privacy*.

Dunque, la normativa, con la riforma della disciplina operata dal D.Lgs. 151/2015 («Riforma Madia»), regola le condizioni di legittimità del controllo e le modalità d'uso delle informazioni raccolte e subordina la possibilità per il datore di avvalersi dei dati così registrati all'adempimento dei predetti oneri.

Tuttavia, soprattutto nell'ambito privato, è emersa negli anni la tendenza da parte dei datori di lavoro, di fronte ad indizi concreti di illeciti in atto da parte dei dipendenti a danno del patrimonio aziendale, di effettuare comunque una sorveglianza occulta sul luogo di lavoro per fugare il dubbio sulla sussistenza o meno di tali condotte, anche senza aver preventivamente dato corso ai necessari adempimenti imposti dall'art. 4 dello Statuto dei lavoratori. Sul punto, si scontrano quindi due esigenze contrapposte: da un lato, quella dell'impresa di prevenire la commissione di reati e di avviare a sorpresa e in segretezza indagini interne a tutela del patrimonio aziendale; dall'altro, quella legata al divieto di elusione dalla disciplina giuslavoristica in tema di controllo a distanza dei lavoratori e alla necessaria protezione del lavoratore rispetto a forme di sorveglianza generalizzata (e incontrollata)[248]. La Corte di Cassazione, con sentenza n. 4746/2002, aveva cercato di trovare un bilanciamento tra i due interessi, giungendo alla conclusione per cui, «ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori […], è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cd. controlli difensivi)». Ritenuti ammissibili i controlli difensivi, questi però devono essere effettuati secondo i canoni generali della correttezza e della buona fede contrattuale, cioè nel rispetto dei principi di ragionevolezza e proporzionalità (quindi, la sorveglianza occulta, a queste condizioni, non vìola l'art. 8 CEDU)[249]. Infine, sul punto si è espressa la Grande Camera della Corte EDU nel caso López Ribalda[250], confermando la legittimità della sorveglianza occulta in assenza del previo rispetto degli

[248] Sul tema della *privacy* in ambito giuslavoristico, si veda C. PISANI – G. PROIA – A. TOPO (a cura di), Privacy *e lavoro. circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Francis Lefebvre, Milano 2022; specificamente sui controlli difensivi, si vedano le pp. 348 e ss.

[249] Cfr. Corte di Cassazione, sentenza n. 10636/2017; si fa riferimento alla giurisprudenza della Corte EDU, che ritiene rispettato il diritto al rispetto della vita privata e familiare delle persone di cui all'art. 8 Convenzione EDU quando le modalità con cui è effettuato il controllo sono proporzionate e ragionevoli (Corte EDU, sentenza Bărbulescu c. Romania (ricorso n. 61496/08), 12 gennaio 2016).

[250] Corte EDU, Grande Camera, sentenza López Ribalda e altri c. Spagna (ricorsi nn. 1874/13 e 8567/13), 17 ottobre 2019.

adempimenti imposti dalla disciplina giuslavoristica in tema, a condizione che vi siano concreti indizi tali da segnalare la presenza di illeciti in atto da parte dei dipendenti, il controllo sia effettuato con modalità proporzionate e coerenti con l'unico scopo di accertare gli illeciti in atto e lo stesso accertamento sia interrotto una volta terminata l'indagine (appunto perché non deve tradursi in un significativo controllo sull'ordinario svolgimento dell'attività lavorativa)[251].

Fatta questa panoramica, si possono fare una serie di considerazioni. Anzitutto, i sistemi di *big data analytics* rientrano nella nozione di «altri strumenti dai quali derivi anche la possibilità di controllo a distanza» di cui all'art. 4 L. 300/1970, quindi legittimamente possono essere utilizzati per il fine consentito di «esigenze organizzative», quali sono la necessaria attuazione delle misure di anticorruzione previste, per le pubbliche amministrazioni, nel PTPCT e nel PIAO e, per le aziende, nel modello 231. In secondo luogo, operando questi dispositivi un controllo costante, il loro utilizzo deve essere espressamente previsto nei Piani appena detti e negli atti di autoregolazione societari e adottato in seguito alla sussistenza di un accordo sindacale o, in mancanza, all'autorizzazione dell'Ispettorato territoriale del lavoro. Infine, gli impiegati devono essere adeguatamente informati sulle modalità d'uso degli strumenti e di effettuazione dei controlli.

Per quanto riguarda gli specifici controlli difensivi, è più probabile che l'adozione occulta di sistemi di segnalazione delle anomalie nel caso di sospetti di illecito in merito ad una specifica situazione di criticità (fase *post delictum*) avvenga nel settore privato. Le aziende, infatti, per evitare di incorrere a loro volta in sanzioni penali *ex* D.Lgs. 231/2001 a causa del comportamento assunto dal dipendente, hanno tutto l'interesse (in qualità di potenziale imputato o di persona offesa) a cominciare ad indagare prima dell'avvio di un procedimento penale: attività, quella delle indagini interne, che è disciplinata in modo frammentario e lacunoso[252] e che non sempre può qualificarsi come indagini difensive ai sensi degli artt. 391-*bis* e ss. del codice di rito. Ad ogni modo, tale controllo sarà lecito se effettuato, per il tempo strettamente necessario a svolgere le indagini, con modalità proporzionate e coerenti con l'unico scopo di accertare gli illeciti in atto.

Nel settore pubblico, invece, la fase dei controlli difensivi non rileverebbe, in quanto i dispositivi di IA sarebbero sempre utilizzati ed i dipendenti ne sarebbero messi a conoscenza ai sensi dell'art. 4 dello Statuto dei lavoratori. In tale contesto, il Responsabile della prevenzione della corruzione (RPCT), che viene a conoscenza di fatti che rappresentano notizia di reato, deve semplicemente presentare denuncia alla procura della Repubblica o ad un ufficiale di polizia

[251] In ambito interno, nel solco dell'indirizzo interpretativo della Corte EDU, si vedano, *ex multis*, Corte di Cassazione, Sez. III, sentenza n. 3255/2020 e Corte di Cassazione, Sez. Lavoro, sentenza n. 34092/2021.

[252] In tema, si veda A. NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*, in *Diritto penale contemporaneo*, n. 4/2021, specialmente pp. 103 e ss. (reperibile *online* al collegamento https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_4_2021_nisco.pdf, consultato da ultimo in data 21 giugno 2022).

giudiziaria con le modalità previste dalla legge (art. 331 c.p.p.) e darne tempestiva informazione all'Autorità Nazionale Anticorruzione.

Specificamente per il settore privato, sul nesso tra generale utilizzo di strumentazione tecnologica e indagini interne agli enti nella fase *post delictum*, non si può che sottolineare come non manchino forti rilievi di criticità, soprattutto se si pensa che la normativa di cui all'art. 4 dello Statuto dei lavoratori e le sanzioni previste in caso di utilizzo illegittimo di strumenti di sorveglianza[253] confliggono con gli obblighi di predisporre controlli interni e attuare misure di conformità penale. Come è stato osservato, il fatto che «la non corretta gestione di tali strumenti comporti la possibile contestazione di violazioni penalmente rilevanti, allora, deve indurre a interrogarsi sulla razionalità complessiva di un sistema che, da un lato, chiede all'impresa di investire significative risorse per la prevenzione del rischio reato e, dall'altro, espone chi la gestisce a un rischio punitivo in caso di non conformità a una disciplina che – ci pare sia questo il punto cruciale – è stata pensata ad altri fini dal legislatore, e non certo per regolare le attività di *compliance* penale e le *internal investigation* svolte dagli enti collettivi»[254]. Allo stesso tempo, si sollevano questioni di ammissibilità e utilizzabilità dei risultati investigativi, anche in ragione dell'incerta riconducibilità ad una precisa categoria probatoria: infatti, se, da un lato, «i lavoratori fruiscono di un'ambigua protezione processuale, in quanto l'inutilizzabilità degli elementi probatori ottenuti attraverso i controlli non autorizzati è circoscritta al rapporto di lavoro», dall'altro, gli stessi elementi «potrebbero restare inutilizzati in un procedimento disciplinare attivato a seguito dell'infrazione del modello organizzativo, e nondimeno essere posti alla base dell'accusa (e di un'eventuale condanna) in sede penale»[255].

Ad ogni modo, sulla generale legittimità di utilizzare dispositivi che analizzano il rischio e segnalano anomalie si è già occupato anche il Garante Privacy. Quest'ultimo, nel tentativo di trovare un equilibrio fra la legittima esigenza di lotta all'evasione e la compressione della sfera giuridica del contribuente, ha reso parere positivo[256] in merito alla sperimentazione da parte dell'Agenzia delle Entrate di un *software* per l'analisi del rischio di evasione; nello specifico, il

[253] L'art. 171 Codice Privacy sancisce che la violazione, in particolare, delle regole relative alle condizioni di legittimità del controllo sancite dall'art. 4, co. 1 Statuto dei lavoratori è punita con le sanzioni di cui all'art. 38 dello stesso Statuto (pena alternativa dell'ammenda da 154 a 1549 euro o dell'arresto da 15 giorni ad un anno). In merito della tutela del domicilio informatico del dipendente, il consolidato orientamento della Corte di Cassazione è quello di configurare il reato di accesso abusivo a sistema informatico nel caso di controllo ingiustificato delle e-mail dei dipendenti pubblici e privati.

[254] Così, E. BIRRITTERI, *Controllo a distanza del lavoratore e rischio penale*, in *Sistema penale*, 2021, pp. 5-6 (reperibile *online* al collegamento https://www.sistemapenale.it/it/scheda/cassazione-3255-2021-controllo-distanza-lavoratore?out=print, consultato da ultimo in data 21 giugno 2022).

[255] In questi termini, A. NISCO, *Prospettive penalistiche del controllo a distanza*, op. cit., p. 105.

[256] Garante Privacy, provvedimento n. 58 del 14 marzo 2019 (reperibile *online* al collegamento https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9106329, consultato da ultimo in data 21 giugno 2022).

dispositivo è capace di predisporre degli elenchi selettivi di contribuenti da sottoporre a controllo mediante l'incrocio dei dati contenuti nell'Anagrafe tributaria e nell'Archivio dei rapporti finanziari, quale prodromo alle modalità di accertamento ordinarie. In sede di parere, il Garante Privacy aveva fissato alcuni paletti all'attività di profilazione, tra cui «la necessità di un vaglio successivo a quello automatizzato, nonché la necessità di un contraddittorio con il contribuente»[257].

Mutatis mutandis, i sistemi di IA utilizzati per finalità di anticorruzione dovrebbero essere ammessi ad operare a fronte dell'applicazione di garanzie al trattamento automatizzato dei dati personali, in funzione ancillare dei dirigenti d'area e degli operatori deputati al controllo delle anomalie e con la eventuale previsione per il dipendente segnalato di giustificare in contraddittorio le anomalie riscontrate. Qui il punto non è tanto il pericolo per la *privacy* dei dipendenti o dell'interessato oggetto di controllo per il tramite di questi dispositivi, che il Garante Privacy ritiene appunto lecitamente comprimibile a fronte di certe tutele, ma piuttosto il diritto di difendersi da prove documentali formatesi nel corso delle indagini interne, con relativi rischi di autoincriminazione (in conflitto con il principio *nemo tenetur se detergere*).

A far, comunque, propendere lo scrivente per l'eventualità (e non l'obbligatorietà) del contraddittorio tra controllori interni e dipendente di impresa privata a seguito della segnalazione di un'anomalia da parte del sistema di IA vi sono i principi procedurali appena detti e i suesposti orientamenti giurisprudenziali. Il bilanciamento tra la necessità che i controlli e le indagini si possano svolgere in segretezza per poter essere efficaci ed il dovere di rispettare le disposizioni di cui all'art. 22 GDPR e all'art. 11 Direttiva (UE) n. 2016/680, che vietano decisioni basate unicamente su trattamenti automatizzati, sta nel fatto che, comunque, il risultato dell'elaborazione non può determinare automaticamente una conseguenza nella sfera giuridica dell'interessato: è l'uomo a stabilire come trattare e valutare la segnalazione e quando coinvolgere la polizia giudiziaria o la procura della Repubblica. Il trattamento automatizzato deve costituire un elemento oggetto di una più ampia considerazione da parte del responsabile e non determinare decisioni che di per sé producono effetti giuridici o incidono significativamente sulla vita dell'interessato[258]. Questa ricostruzione non pare avere particolari criticità, almeno per il settore pubblico, in quanto il responsabile che non vigila e vaglia le segnalazioni è destinatario delle sanzioni di cui all'art. 1, cc. 12-13 L. 190/2012; sarà lui a valutare in modo più approfondito se chiedere direttamente conto al dipendente delle anomalie riscontrate e/o se fare ulteriori indagini, prima di avvisare le competenti autorità. Invece, per il settore privato, come si è visto, la ricostruzione sistematica è più complessa e

[257] Così, G. DE PETRIS, *La digitalizzazione del Fisco e la difficile parità delle armi fra Amministrazione e contribuente*, in *Corriere Tributario*, n. 6/2020, p. 589. Cfr. Garante Privacy, provvedimento n. 58/2019 cit., primo "Ritenuto".

[258] Cfr. E. BIRRITTERI, Big Data Analytics *e* compliance *anticorruzione*, op. cit., p. 296.

contraddittoria e ciò non può che portare «il legislatore […] [a] farsi carico dell'esigenza di regolare direttamente tali attività di *compliance* e controllo interno, garantendo sì l'interesse dell'impresa di avvalersi dei più moderni ed efficienti strumenti di prevenzione del reato, ma avendo cura di contenere l'impatto che simili attività producono sui diritti fondamentali dei singoli interessati»[259].

Tra l'altro, nella successiva fase di indagine portata avanti dalle competenti autorità, proprio lo strumento predisposto dall'Agenzia delle Entrate potrebbe aiutare a scovare a carico del dipendente sospettato di corruzione informazioni sulla possibile ricezione di tangenti o favori, in quanto si concentra proprio a segnalare disallineamenti tra le disponibilità finanziarie risultanti dalle informazioni comunicate all'archivio dei rapporti finanziari e i ricavi/volume d'affari dichiarati.

Tuttavia, specificamente nel settore privato, queste analisi informatiche dei dati potranno essere soltanto strumenti di mera valutazione del rischio ove l'azienda decida, in un secondo momento, di controllare il proprio patrimonio informativo per identificare aree sensibili ed esposte al verificarsi di illeciti, senza rendere tali strumenti parte integrante dei protocolli operativi di controllo del rischio reato. In tal caso, l'IA verrebbe utilizzata *una tantum* per identificare i punti deboli e adottare correttivi volti al miglioramento futuro della conformità interna dell'azienda. Nel caso in cui, invece, l'azienda volesse dotarsi dell'IA per fini di valutazione e gestione del rischio, potrà prevederne l'applicazione nei protocolli operativi di gestione del rischio corruzione, sulla scorta di quanto ipotizzato sopra per le PA con il PTPCT e il PIAO. «Ciò, nella prassi, accade principalmente rispetto alle procedure di c.d. due diligence nei confronti di terze parti, ove ogni procedura decisionale in merito all'opportunità di intraprendere un determinato affare è anticipata dalle predette attività di *data analytics*, con la previsione di un *report in real time* al *management* in merito alle eventuali anomalie rilevate e ai conseguenti rischi legali e di non conformità connessi ai possibili rapporti da intraprendere con il singolo partner/agente commerciale (specie per affari all'estero rispetto ai quali può esistere un rischio di corruzione internazionale»[260].

In conclusione, viste le potenzialità che gli strumenti di *big data analytics* avrebbero nello svolgere attività di segnalazione del rischio e delle anomalie, la necessità di tutelare il diritto alla *privacy* delle persone oggetto di controllo di fronte ad attività di sorveglianza illecite e sproporzionate e l'esigenza di fornire delle indicazioni chiare alle imprese che volessero fare un uso costante o saltuario di tali dispositivi di IA per le varie finalità dette (indagini difensive, *risk assessment* e *risk management*), si rende assolutamente necessario che il legislatore, quanto prima, regoli la materia, bilanciando correttamente i diversi interessi in gioco e dando misure chiare, di modo da rendere l'utilizzo dell'IA per finalità anticorruzione una realtà quotidiana.

[259] In questi termini, E. BIRRITTERI, *Controllo a distanza del lavoratore*, op. cit., p. 6; Cfr. E. BIRRITTERI, Big Data Analytics *e* compliance *anticorruzione*, op. cit., p. 297.

[260] Così, E. BIRRITTERI, Big Data Analytics *e* compliance *anticorruzione*, op. cit., pp. 294-295.

CAPITOLO III

LE PROVE DIGITALI: RIVERBERI PROCESSUALI E VALENZA PROBATORIA

SOMMARIO: 3.1 Il sistema probatorio di fronte alla prova digitale. – 3.2 La prova digitale in rapporto al diritto al rispetto della vita privata. – 3.2.1 I parametri convenzionali per una legittima compressione del diritto alla *privacy*. – 3.2.2 Violazione della *privacy* e conseguenze sul piano del rispetto dell'equo processo. – 3.3 La prova digitale e i rischi per la parità delle armi. – 3.4 Sull'utilizzabilità processuale dei risultati investigativi ottenuti mediante sistemi automatici.

3.1 Il sistema probatorio di fronte alla prova digitale.

Oltre alla fase della prevenzione, nella quale sta crescendo l'impiego di strumenti di polizia predittiva e di identificazione di profili di anomalia, altri due ambiti nei quali l'IA si sta sviluppando in «modo tumultuoso» sono «quello strettamente probatorio, delle c.d. *automated* o *digital evidence*[1]» (come visto, «nella fase delle indagini, si fa un uso sempre più ampio di sistemi basati su prove algoritmiche in senso lato») e «quello della […] "giustizia predittiva"[2]»[3].

Nelle pagine che seguiranno, ci si concentrerà sulla valenza probatoria che potrebbe essere riconosciuta alle risultanze dell'elaborazione di strumentazione digitale ottenute durante le fasi di prevenzione e di indagine.

La categoria delle prove digitali[4], quale sottoinsieme della prova tecnologica e scientifica, che già nel momento della sua irruzione nel processo aveva determinato la necessità per il giudice di domandarsi a quali condizioni un'informazione potesse essere alla base di un provvedimento perché ritenuta dotata di validità scientifica, ha fatto nuovamente sorgere dei problemi, ravvivando il tema dell'ingresso di nuove tecnologie e saperi scientifici nel procedimento probatorio. Infatti, le prove digitali (*digital evidence*) sia tradizionali (cioè la «prova informatica [acquisita] nell'ambito e

[1] Sul tema tra IA e prova penale, si veda il lavoro pionieristico di L. LUPÁRIA, *Prova giudiziaria e ragionamento artificiale: alcune possibili chiavi di lettura*, in J. SALLANTIN – J.-J. SZCZECINIARZ (a cura di), *Il concetto di prova alla luce dell'intelligenza artificiale*, Giuffrè Editore, Milano 2005, pp. VII-XXVI.

[2] Sulla giustizia predittiva nell'ambito strettamente penale, si veda, oltre a quanto già segnalato *supra*, D. POLIDORO, *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *Archivio penale*, n. 3/2020, pp. 12 e ss. (reperibile *online* al collegamento https://archiviopenale.it/File/DownloadArticolo?codice=8f90d1bc-acef-4725-8fd3-c256a7934831&idarticolo=25993, consultato da ultimo in data 21 giugno 2022).

[3] Per tutte le citazioni presenti in questo capoverso, si veda M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, op. cit., p. 2.

[4] Sul tema della prova digitale, si vedano, *ex multis*, L. LUPÁRIA – G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano 2007, spec. pp. 49 e ss. e 141 e ss; M. DANIELE, *La prova digitale nel processo penale*, op. cit., pp. 283 e ss. Lo sviluppo tecnologico a cui si assiste quotidianamente fa sorgere nuovi quesiti e dubbi sulla legittimità e i limiti dell'utilizzo di determinata strumentazione per fini di prevenzione e repressione penale che negli stessi testi citati (un po' datati) non erano nemmeno pensabili e discutibili.

in vista del procedimento penale»[5] attraverso strumentazione digitale[6]) sia basate sulla risultante dell'elaborazione di un dispositivo di intelligenza artificiale[7] sono caratterizzate da forte invasività e possono porsi in tensione sistematica rispetto al diritto alla *privacy* e alle garanzie del giusto processo.

Generalmente, le difficoltà che emergono, in sede di valutazione degli elementi di prova a matrice scientifica, conseguono all'evoluzione che ha avuto il concetto di scienza nel corso degli anni. In breve, in un primo momento nel quale la scienza era ritenuta infallibile, il perito era considerato l'unico in grado di capire e spiegare come si fossero svolti i fatti oggetto d'indagine e il giudice non poteva far altro che prendere atto della legge scientifica introdotta nel processo dal primo, accogliendo *in toto*, in sede di valutazione della prova tecnica, quanto contenuto nella relazione peritale. Invece, con il successivo venir meno del concetto di infallibilità della scienza e il conseguente imporsi di una valutazione dei fatti in termini probabilistici, il perito è divenuto una sorta di testimone esperto che richiama una legge scientifica per ricostruire il fatto storico oggetto dell'imputazione e in capo al giudice – in analogia con quanto avviene con le fonti di prova tradizionali e alla stregua del tradizionale modello della motivazione – è tornato l'onere di esporre il ragionamento logico-giuridico che ha determinato l'adesione ad una specifica legge di copertura per giungere ad una decisione su un caso specifico. In tale contesto, il contraddittorio tra le parti integra lo strumento principe per assumere la prova scientifica sottoposta a procedure di controllo e falsificazione, permettendo al giudice di interrogarsi sui presupposti di validità dei metodi scientifici utilizzati e sulla loro complessiva coerenza con i fatti di cui si discute[8]. Infatti, «il giudice, al fine di accertare […] l'affidabilità e la validità scientifica di una data teoria e, soprattutto, la sua rilevanza rispetto al fatto contestato nell'imputazione, dovrà compiutamente valutare: la controllabilità e falsificabilità della teoria di specie; la conoscenza del tasso di errore che ne caratterizza le implicazioni; la sottoposizione di essa al controllo della comunità scientifica; la generale accettazione di essa presso la comunità degli esperti»[9].

---

[5] Così, A. ZIROLDI, *Intelligenza artificiale e processo penale*, op. cit., p. 10.

[6] Si pensi, ad esempio, all'impiego del captatore informatico.

[7] Come era già stato precisato, si ricorda che la tecnologia digitale diventa intelligenza artificiale solo se è programmata per riprodurre almeno una delle capacità cognitive degli esseri umani.

[8] Il problema della falsificabilità del sapere tecnico introdotto nel processo penale è testimoniato, appunto, dall'abbandono della concezione di infallibilità della perizia. In merito, la Cassazione penale, Sez. un., sentenza n. 14426/2019, facendo riferimento alle sentenze «Cozzini» (si veda nota subito oltre) e «Franzese», ha sottolineato «il ruolo decisivo, che, nell'ambito della dialettica processuale, assume il contraddittorio orale attraverso il quale si verifica, nel dibattimento, l'attendibilità del perito, l'affidabilità del metodo scientifico utilizzato e la sua corretta applicazione alla concreta fattispecie processuale […], operazioni tutte che consentono anche di distinguere le irrilevanti o false opinioni del perito (cd. *junk science*) dai pareri motivati sulla base di leggi e metodiche scientificamente sperimentate ed accreditate dalla comunità scientifica» (*Considerato in diritto*, par. 5.1).

[9] In questi termini, G. RANALDI, *Processo penale e prova informatica: profili introduttivi*, in *Diritto Pubblico Europeo Rassegna* online, n. 2/2020, p. 6 (reperibile *online* al collegamento http://www.serena.unina.it/index.php/dperonline/article/view/7031, consultato da ultimo in data 21 giugno 2022). La

Oggi, invece, il fatto che dispositivi digitali o di intelligenza artificiale possano, attraverso l'enorme quantità di dati elaborati, fornire anche elementi conoscitivi rilevanti per stabilire la responsabilità penale in capo ad un soggetto ha portato gli addetti ai lavori a riflettere sull'ammissibilità e utilizzabilità di tali dati nel procedimento penale e, soprattutto, ha sollevato nuove problematiche in tema di efficienza tecnologica come criterio autosufficiente di attendibilità della prova.

La capacità degli algoritmi di generare e trattare automaticamente dati con finalità di prevenzione e repressione penale non può che avere delle conseguenze all'interno del procedimento penale, non solo per il rapporto che si viene a creare tra l'IA e la prova penale, ma anche per i diritti potenzialmente lesi a seguito dell'impiego di tali strumenti tecnologici. Sul punto, si pensi sia ai dati ottenuti attraverso strumenti digitali di captazione occulta, rilevanti per le indagini e la prova dei fatti oggetto di imputazione, sia ai dati prodotti in autonomia da un algoritmo installato in un apparecchio (ad esempio, un elettrodomestico o le scatole nere delle autovetture a guida automatizzata) che potrebbero essere utilizzati (in favore tanto dell'accusa quanto della difesa)[10], quale la presenza o meno dell'indagato o dell'imputato sul luogo del delitto[11]. Tra l'altro, oltre a rilevare come elementi rappresentativi che possono essere acquisiti a processo come documenti (art. 234 c.p.p.)[12], le prove digitali rilevano quale risultato dell'attività di strumentazioni che hanno

---

specifica elencazione è stata enucleata dalla giurisprudenza italiana, che ha individuato specifici criteri ermeneutici in grado di orientare il giudice in sede di valutazione delle diverse teorie scientifiche. Cfr. Cassazione penale, Sez. IV, sentenza n. 43786 (sentenza «Cozzini»), 17 settembre 2010, in analogia con quanto chiarito dai giudici statunitensi in Supreme Court of the United States, *Daubert v. Merrel Dow Pharmaceuticals, Inc*., 509 US 579, 28 giugno 1993. I cd. criteri Daubert stabiliscono le condizioni alle quali il giudice deve vagliare l'effettiva affidabilità di una teoria o un metodo e di un perito (*expert testimony*), ai fini della loro ammissibilità come prova scientifica nel processo: la controllabilità mediante esperimenti; la falsificabilità mediante esame di smentita con esito negativo; la recensione da parte dei pari grado (*peer review*) della comunità scientifica di riferimento; la conoscenza della percentuale di errore dei risultati; infine, il criterio subordinato e ausiliario della generale accettazione da parte della comunità degli esperti. La Corte di Cassazione italiana ha, appunto, fatti propri i *Daubert standard*, arricchendone la portata, con riguardo alla fase della valutazione della prova scientifica da parte del giudice, aggiungendo i criteri dell'indipendenza e dell'affidabilità dell'esperto, l'ampiezza e il rigore del dibattito critico che hanno accompagnato la ricerca, le finalità e gli studi che la sorreggono e l'attitudine esplicativa dell'elaborazione teorica.

[10] Da ciò deriva la necessità di formare tecnicamente gli addetti di P.G. che acquisiscono e conservano i dati digitali, per evitare che comportamenti scorretti possano incidere gravemente sul piano dell'accertamento giudiziale. Al riguardo, si può menzionare il caso «Stasi». Sull'esigenza di preservare integrità e genuinità dei dati digitali raccolti in sede di indagini, cfr. S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 124 e ss. Tra l'altro, con la L.48/2008, norma con la quale lo Stato Italiano ha ratificato Convenzione di Budapest del 2001 del Consiglio d'Europa sulla criminalità informatica, sono stati posti i pilastri per la prova digitale disciplinando alcuni aspetti relativi a: consentire la conservazione dei dati originali; impedirne l'alterazione nel corso delle operazioni di ricerca delle fonti di prova; garantire la conformità della copia con l'originale nonché l'immodificabilità quando si proceda ad una duplicazione; dotare di sigilli informatici i documenti appresi.

[11] Per l'esempio, cfr. S. QUATTROCOLO, *Equità del processo penale*, op. cit., p. 117. Tra l'altro, la verifica dell'alibi informatico sta diventando sempre più problematica a causa dell'utilizzo da parte della criminalità di specifici *softwares* che, permettendo al *computer* di svolgere automaticamente delle operazioni, simulano un'attività umana, pur in assenza del soggetto a cui si vorrebbe riferita. In tema, si veda V. CALABRÒ – G. COSTABILE – S. FRATEPIETRO – M. IANULARDO – G. NICOSIA, *L'alibi informatico. Aspetti tecnici e giuridici*, in *IISFA Memberbook*, Experta, Forlì 2010, pp. 297-328 (reperibile *online* al collegamento https://www.vincenzocalabro.it/pdf/2010/AlibiInformatico.pdf, consultato da ultimo in data 21 giugno 2022).

[12] I documenti sono prove rappresentative di un fatto formate al di fuori del processo nel quale si chiede o si dispone

incrementato le potenzialità dei tradizionali mezzi di indagine.

Si pensi ad apparecchi digitali[13] per effettuare videoriprese[14], intercettazioni di comunicazioni[15], intercettazioni informatiche, il pedinamento geospaziale (attraverso il rilevatore GPS)[16] e il monitoraggio dei dispositivi elettronici presenti in un certo raggio di azione (per mezzo di *IMSI Catcher*)[17] o agli algoritmi di polizia predittiva in grado di procedere al riconoscimento facciale[18], mettendo a confronto il volto di uno sconosciuto (rappresentato in una fotografia o ripreso in un video) con una o più immagini (contenute in banche dati) di volti di soggetti già noti, che, proprio per questa maggiore capacità elaborativa, possono avere una ricaduta diretta all'interno del processo penale.

La questione è capire quale possa essere la sorte processuale degli eventuali elementi di prova raccolti a seguito dell'impiego di *software* di IA in attività di prevenzione e di indagine. Le segnalazioni che fossero trasfuse in un documento da parte degli addetti di polizia, dei responsabili della prevenzione della corruzione o dei funzionari addetti ai controlli (si pensi ai controlli effettuati dall'Agenzia delle Entrate attraverso il dispositivo sopra descritto) possono essere poste alle base di un di un successivo intervento volto a determinare, con metodi tradizionali, l'accertamento di un reato. Il problema si pone, invece, quando gli elementi indiziari contenuti nella relazione della macchina potrebbero rilevare direttamente per il procedimento penale.

Come è stato osservato, anche se limitatamente all'attività di polizia predittiva, quest'ultima «impedisce, nel caso di specie, la commissione di un reato (o lo "limita" alla forma del tentativo). In che termini l'insieme di elementi tratti dal data base del programma possono "entrare" – in esito all'elaborazione – in un'annotazione di p.g. finalizzata – al contrario – a una richiesta di misura

---

che essi facciano ingresso. Le prove documentali sono ammesse nel processo quando il documento risulta materialmente formato fuori, ma non necessariamente prima, del procedimento e l'oggetto della documentazione appartiene al contesto del fatto oggetto di conoscenza giudiziale e non al contesto del procedimento. Gli elementi raccolti nel corso delle indagini con atti investigativi effettuati nel corso delle stesse costituiscono la documentazione dell'attività investigativa e non documenti.

[13] Per una breve panoramica su tali strumenti, si veda S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., pp. 63-67.

[14] Sulle videoriprese, si vedano, *ex multis*, A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cassazione penale*, 1999, pp. 1192-1213; ID., *Captazione di immagini (diritto processuale penale)*, in *Enciclopedia del diritto. Annali, vol. VI*, Giuffré, Milano 2013, pp. 133-149; ID., *Le Sezioni Unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni nuovi dubbi*, in *Rivista italiana di diritto e procedura penale*, 2006, pp. 1550-1569; V. BONINI, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in *Processo penale e giustizia*, n. 2/2019, pp. 338-348 (reperibile *online* al collegamento http://images.processopenaleegiustizia.it/f/articoli/591_articolo_dnHay_ppg.pdf, consultato da ultimo in data 21 giugno 2022).

[15] In tema, A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Rivista italiana di diritto e procedura penale*, n. 2/2005, pp. 594-650.

[16] Per un'analisi del rilevatore GPS, si veda S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Rivista italiana di diritto e procedura penale*, n. 2/2012, pp. 580-607.

[17] Sul cacciatore di IMSI (*International Mobile Subscriber Identity*), brevemente, W. NOCERINO, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Prima parte)*, op. cit., pp. 826-827.

[18] Sul legame tra *software* di polizia predittiva per il riconoscimento facciale (SARI) e processo, approfonditamente, M. TORRE, *Nuove tecnologie e trattamento dei dati personali*, op. cit., pp. 1042-1056.

cautelare o, poniamo, di una richiesta di intercettazione o quale elemento di prova al fine dell'esercizio dell'azione penale? In che modo potranno essere, tali elementi e soprattutto le interconnessioni individuate, utilizzat[i] in sede dibattimentale? Che tipo di valutazione è "accettabile" per il sistema penale in relazione a tali esiti? In questa prospettiva, la verifica deve avvenire su piani differenti. In primo luogo è indispensabile che tutti gli elementi inseriti nella banca dati siano stati acquisiti – sia per le forme, sia per i termini temporali – in ossequio alle indicazioni codicistiche. [...] Se nell'ottica della polizia di prevenzione, ferme restando eventuali responsabilità (penali e/o disciplinari) per le singole condotte dirette ad acquisire elementi al di fuori dei termini di legge, tutto il materiale acquisito e analizzato "serve" per ottenere la prevenzione di reati, per la polizia giudiziaria solo gli elementi acquisiti in termini sintonici alla disciplina codicistica potranno essere correttamente e completamente utilizzati. O, quantomeno, solo quelli che potranno essersi "formati" senza incorrere in un formale divieto di utilizzabilità (art. 191 c.p.p.). Sul piano metodologico, […] [g]li elementi storici che sono posti alla base delle comparazioni e della ricerca di correlazioni, devono potere – in astratto – essere singolarmente e autonomamente portati all'attenzione del Tribunale (o del GIP in fase di indagine). Le singole immagini che ritraggano, in ipotesi, il medesimo cappellino indossato durante le rapine o le dichiarazioni di persone informate che descrivono le frasi e la corporatura di un autore di rapine seriali potrebbero […] essere oggetto di "ostensione" al Tribunale (nel primo caso) e oggetto di testimonianza (o di valutazione nell'ambito di un verbale, in fase di indagine) nel secondo caso?»[19].

Queste osservazioni, a parere di chi scrive, possono essere riferite a tutte le attività di prevenzione di cui si è discusso finora. Ciò non significa, però, contraddire quanto affermato in più occasioni sulla necessità, in ambito penale, di limitare l'uso dell'intelligenza artificiale a un ruolo ancillare e di ausilio alle attività umane: infatti, tanto gli strumenti di polizia predittiva quanto i dispositivi di indicazione del rischio come i *big data analytics* (in ambito sia anticorruzione sia fiscale)[20], ai sensi dell'art. 11 della Direttiva (UE) n. 2016/680, non potranno mai produrre effetti penali diretti nella sfera giuridica dell'interessato, se non nelle situazioni dette (autorizzazione del

[19] In questi termini, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., pp. 58-59. Sul punto, è stato appunto osservato che «non tutti i *tools di predective policing* risultano indifferenti al processo penale», ove si considerino, per esempio, quelli che si basano anche sul «riconoscimento facciale»; così, G. RICCIO, *Ragionando su intelligenza artificiale e processo penale*, in *Archivio penale*, n. 3/2019, p. 7 (reperibile *online* al collegamento https://archiviopenale.it/File/DownloadArticolo?codice=ec8503fc-df47-4c00-bdad-28b70ffd50f7&idarticolo=21741, consultato da ultimo in data 21 giugno 2022).

[20] Come indicato, il trattamento automatizzato deve costituire un elemento oggetto di una più ampia considerazione: dunque, le elaborazioni degli algoritmi di polizia predittiva devono sempre essere vagliate dagli addetti di polizia; le segnalazioni degli indicatori di anomalia devono essere comunicate alle autorità preposte, per permettere loro di raccogliere eventuali altri elementi a carico della persona controllata; analogamente, a seguito dell'attività di profilazione fiscale, devono essere previste «una puntuale valutazione della coerenza complessiva della posizione di ciascun contribuente selezionato da parte di operatori qualificati […] preliminare alla convocazione del contribuente» e una fase di contraddittorio (così, cfr. Garante Privacy, provvedimento n. 58/2019 cit., primo "Ritenuto").

diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e previsione di garanzie) e a fronte di un intervento umano "qualificato" e attivo; ciò non preclude, però, l'utilizzo degli elementi elaborati dalla macchina nell'ambito del procedimento penale, nel momento in cui ne ricorrano le condizioni[21].

Quindi, come organizzare l'accesso nel contesto processuale di questo tipo di prove digitali? Come assicurare che sulla prova così acquisita trovi spazio il diritto di difesa, attraverso il confronto dialettico, la confutazione, la prova contraria, il dubbio? Come garantire il contraddittorio "sulla" prova, in funzione della validazione scientifica del risultato probatorio e contro il rischio di un'autosufficienza euristica discendente dal grado più o meno elevato di condivisione sociale dei risultati della tecnologia?[22] Il risultato dell'elaborazione potrà essere considerato un indizio rilevante ai sensi dell'art. 192 c.p.p., per il quale l'«esistenza di un fatto non può essere desunta da indizi a meno che questi siano gravi, precisi e concordanti»?

Tra l'altro, l'interprete, cercando di disciplinare tutti questi aspetti nell'ottica di garantire la tenuta del sistema penale, deve mantenere in equilibrio diverse esigenze, quali l'interesse-dovere pubblico all'accertamento dei fatti e la necessità di tutelare i diritti individuali: infatti, «il bilanciamento tra opposte esigenze deve essere individuato secondo criteri di proporzionalità e ragionevolezza, tali, da un lato, da salvaguardare il "nucleo essenziale" del diritto e, dall'altro lato, da consentire, entro certi limiti, l'impiego di nuovi strumenti investigativi in grado di fornire un contributo importantissimo alle indagini»[23]. Il riferimento, qui, è al diritto alla *privacy* e al diritto ad un equo processo. Il primo viene leso dal potenziale intrusivo di certi dispositivi digitali e di intelligenza artificiale di cui possono usufruire le autorità inquirenti; il secondo, invece, rileva perché, la spendibilità processuale dei risultati ottenuti mediante questi strumenti investigativi, sia in termini di utilizzabilità, sia in termini di attendibilità della prova, si scontra con il tradizionale diritto probatorio.

---

[21] Sul punto, Mario Venturi, l'inventore dell'algoritmo di polizia predittiva KeyCrime, sostiene che non sia necessario sottoporre a trasparenza e controllo l'algoritmo stesso perché «*non ha valenza scientifica in sede processuale*» (cfr. A.D. SIGNORELLI, *Il software italiano*, op. cit., ultimo capoverso). Da un lato, tale considerazione può essere accettabile, se si accoglie la spiegazione per cui «*il software ti propone solo il crime linking e la predizione dei prossimi obiettivi*», dunque è mero «*tassello*» di un successivo *iter* investigativo svolto secondo canoni tradizionali. Dall'altro lato, però, non si può non notare come la stessa spiegazione sia stata utilizzata – e vada limitata – per giustificare la mancata sottoposizione del dispositivo a controllo esterno: infatti, il fatto che il collegamento criminale sia scovato da un algoritmo risolleva la questione di come utilizzare le risultanze algoritmiche in sede di procedimento penale. Dal punto di vista probatorio, quindi, anche gli elementi riportati da KeyCrime possono essere posti all'attenzione del giudice durante le indagini o in sede processuale, contrariamente a quanto sostenuto da Venturi (sul piano della trasparenza). In questo caso specifico e negli altri, quindi, una soluzione sul da farsi non può essere indicata a priori in astratto, ma, di volta in volta, in concreto.

[22] Cfr. G. CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in www.sistemapenale.it, 8 gennaio 2021, par. 4 (reperibile *online* al collegamento https://www.sistemapenale.it/it/articolo/canzio-intelligenza-artificiale-algoritmi-giustizia-penale, consultato da ultimo in data 21 giugno 2022).

[23] Così, M. TORRE, *Nuove tecnologie e trattamento dei dati*, op. cit., p. 1043.

3.2 La prova digitale in rapporto al diritto al rispetto della vita privata.

L'intrusività dei nuovi strumenti tecnologici investigativi nella vita privata degli indagati e dei soggetti sottoposti a procedimento penale, ma anche di terzi estranei che, casualmente, sono oggetto delle loro elaborazioni solo per il fatto di trovarsi in un determinato arco spazio-temporale, genera frizioni con il diritto al rispetto della vita privata, di cui all'art. 8 CEDU; addirittura, tali dispositivi di captazione e di raccolta di informazioni sono così invasivi da caratterizzarsi per un'insidiosità molto più elevata di quella propria degli strumenti tradizionali di intercettazione[24]. Sul punto, in uno studio commissionato dalla Commissione LIBE del Parlamento europeo in materia di intrusioni investigative[25] risulta chiaro come sia necessario trovare un bilanciamento tra i benefici che si possono trarre dall'utilizzo di questi apparati tecnologici e la demarcazione di un limite inviolabile della *privacy*: infatti, *«[a]lthough the use of hacking techniques will bring improvements in investigative effectiveness, the significant amount and sensitivity of data that can be accessed through these means acts as a stimulus for another key debate: ensuring the protection of the fundamental right to privacy*»[26].

Sul piano nazionale, non è rinvenibile nella Carta costituzionale alcuna esplicita menzione del diritto alla *privacy* della persona. Tale scelta dei costituenti va ravvisata nell'originaria nozione di *privacy* quale "diritto di non ingerenza nella sfera privata ad opera dell'autorità pubblica", ricavabile, ad esempio, dagli artt. 14, 15 e 21 Cost., riguardanti rispettivamente l'inviolabilità del domicilio, la segretezza e riservatezza delle comunicazioni e la libertà di pensiero e di parola. Affermato il nocciolo dei diritti, il legislatore[27] avrebbe successivamente disciplinato le circostanze nelle quali l'autorità pubblica fosse autorizzata a limitarlo.

Successivamente, dopo che il diritto è stato declinato secondo linee di segretezza (il fine è evitare che terze persone possano conoscere determinate vicende personali) e riservatezza (volta a vietare la divulgazione di informazioni da parte di chi legittimamente ne è a conoscenza) in senso stretto, sul piano sovranazionale, la *privacy* ha assunto una dimensione positiva, attraverso il riconoscimento all'individuo anche del diritto di controllare la raccolta e il trattamento di

---

[24] Cfr. M. DANIELE, *La prova digitale nel processo penale*, op. cit., p. 288, secondo cui «[l]a loro capacità lesiva della *privacy* è addirittura superiore a quella delle intercettazioni».

[25] Parlamento Europeo – Commissione per le libertà civili, la giustizia e gli affari interni (LIBE), *Legal frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, Marzo 2017 (reperibile *online* al collegamento https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf, consultato da ultimo in data 21 giugno 2022).

[26] Tradotto: «anche se l'uso di tecniche intrusive porterà miglioramenti nell'efficacia investigativa, la significativa quantità e sensibilità di informazioni che possono essere accessibili attraverso questi mezzi funge da stimolo per un altro dibattito chiave: garantire la tutela del diritto fondamentale alla *privacy*». *Idem*, p. 21.

[27] Nel rispetto della riserva di legge assoluta, relativa o rinforzata che si può riscontrare nelle varie disposizioni costituzionali.

informazioni sul proprio conto. Da una parte, l'art. 16 TFUE ha previsto «il diritto di ogni persona alla protezione dei dati di carattere personale»; dall'altra, gli artt. 7 e 8 Carta di Nizza hanno riconosciuto ad ogni persona il diritto «al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni» e il «diritto alla protezione dei dati di carattere personale»[28].

Infine, il diritto alla *privacy* è stato esplicitamente affermato dall'art. 8 CEDU, che, pur senza distinguere tra i concetti di rispetto alla vita privata (inizialmente riconducibile a luoghi e contesti oggettivamente localizzati) e protezione dei dati, ha stabilito un sistema di bilanciamento tra il «diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza» (art. 8 par. 1) e altre esigenze di interesse comune come la sicurezza nazionale, la pubblica sicurezza, il benessere economico del paese, la difesa dell'ordine e la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui, che, nel caso di espressa previsione legislativa, autorizzano la pubblica autorità a procedere alla compressione della *privacy* nell'ambito di quelle misure necessarie, in una società democratica, ad ottenere uno dei fini appena detti (art. 8 par. 2).

Nell'ambito interno, si è cercato di individuare il fondamento del diritto alla *privacy* nell'art. 2 Cost., facendolo rientrare nella clausola aperta, ma priva di garanzie, dei «diritti inviolabili dell'uomo» che la Repubblica riconosce. Tuttavia, a prescindere dal dibattito sulla questione, con le "sentenze gemelle" del 2007 della Corte costituzionale (sentenze nn. 348/2007 e 349/2007), che hanno chiarito l'incidenza nell'ordinamento interno delle norme della Convenzione EDU, non sembra più contestabile che il diritto alla *privacy* sia ascrivibile al novero dei diritti fondamentali dell'ordinamento attraverso la norma interposta dell'art. 8 CEDU.

L'elaborazione giurisprudenziale della Corte di Strasburgo[29], inizialmente imperiata sui concetti fisici di domicilio e corrispondenza, ha fatto confluire nella cornice normativa dell'art. 8 anche la raccolta, l'elaborazione e la profilazione dei dati personali effettuata durante plurime attività (registrazione dei dati esteriori delle comunicazioni, schedatura e archiviazione, ecc.), stabilendo, di fronte a queste nuove forme di intrusione nella vita privata dei cittadini, «un substrato di principi e regole comuni per l'utilizzo per finalità di natura penale dei dati personali e della loro elaborazione»[30]; analogamente, ha enucleato in termini digitali i concetti di corrispondenza e

[28] Sugli artt. 7 e 8 della Convenzione europea dei diritti dell'uomo, brevemente, cfr. S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., pp. 52-56.

[29] Per una panoramica dello sviluppo dell'elaborazione giurisprudenziale della Corte EDU, che con varie sentenze ha allargato la portata dell'art. 8 della Convenzione, si veda Corte europea dei diritti dell'uomo, *Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo. Diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza*, aggiornata al 31 agosto 2019 (reperibile *online* al collegamento https://www.echr.coe.int/documents/guide_art_8_ita.pdf, consultato da ultimo in data 21 giugno 2022).

[30] Così, S. QUATTROCOLO, *Equità del processo penale*, op. cit., p. 112.

domicilio, che, «architravi delle garanzie costituzionali contro le interferenze statuali, anche investigative, nella sfera personale degli individui, [avevano] perso significato di fronte alla possibilità di produrre, scambiare, conservare – ma anche carpire, intercettare, copiare – dati immateriali in uno spazio che non è più quello fisico»[31].

3.2.1 I parametri convenzionali per una legittima compressione del diritto alla *privacy*.

Dunque, l'uso di tecnologie digitali per intercettare dati della vita privata degli individui, non è una pratica vietata dalla Convenzione EDU, a condizione che ricorrano specifiche necessità e vi sia un'espressa previsione di legge.

Il primo requisito della necessità ricorre quando l'obiettivo che si intende raggiungere con l'intrusione medesima è meritevole di tutela e parametrato allo specifico caso preso in considerazione. Tale criterio risulta però soggettivo e non specifico ed ha spinto la Corte EDU a oggettivizzarne i limiti, prevedendo un esame di proporzionalità[32] da effettuare tra il caso specifico e la necessità pubblica lì rilevante. Ciò si traduce per l'autorità pubblica nel dovere di verificare che lo stesso scopo sia raggiungibile senza invadere la sfera privata dell'interessato (principio di sussidiarietà), che diventa così *extrema ratio* a cui giungere con una rigorosa applicazione del principio di proporzionalità (o adeguatezza); allo stesso modo, se l'intrusione è inevitabile, dovrà essere utilizzata la strumentazione in grado di conseguire l'obiettivo prefissato con un grado minore di invasività nella sfera privata della persona oggetto del controllo.

Invece, per quanto riguarda il requisito della previsione per legge, questa deve risultare accessibile e prevedibile: in pratica, la Corte EDU è giunta alla conclusione per cui «la legislazione nazionale deve essere sufficientemente determinata, ossia enunciata con un grado di precisione tale da permettere all'individuo di orientare la propria condotta; al tempo stesso il diritto interno deve fornire una tutela adeguata contro eventuali arbitri e deve definire in modo netto le modalità di esercizio del potere conferito alle autorità competenti»[33]. Inoltre, i dati personali devono essere

---

[31] In questi termini, S. QUATTROCOLO, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in www.medialaws.eu (*Rivista di diritto dei media*), n. 3/2020, pp. 125-126 (reperibile *online* al collegamento https://www.medialaws.eu/wp-content/uploads/2020/12/RDM-3-2020-Quattrocolo-121-135.pdf, consultato da ultimo in data 21 giugno 2022).

[32] Sul principio di proporzionalità espresso dall'art. 8 CEDU e operante in punto di risorse probatorie incidenti sulla *privacy* della persona, si veda, *ex multis*, F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico*, op. cit.

[33] Così, G.M. BACCARI – C. CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla* privacy*: uno sguardo d'insieme*, in *Diritto penale e processo*, n. 6/2021, pp. 712-713; secondo l'impostazione della Corte EDU si possono trarre i principi della prevedibilità, che non significa certezza, della legislazione nazionale e di accessibilità, per il quale devono essere chiari i poteri dell'autorità pubblica e previsti dei meccanismi per contestare un eventuale atteggiamento che andasse oltre i limiti stabiliti. Cfr. Corte EDU, *Uzun v. Germany* (ric.35623/05), 2 settembre 2010, par. 63 (sentenza reperibile *online* al collegamento https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22uzun%22],%22documentcollectionid2%22:[%22GRANDCHAM

pertinenti e non eccessivi rispetto alla finalità per le quali sono raccolti, venendo trattati per il tempo strettamente necessario a portare a termine l'attività di intrusione nella *privacy* dell'interessato[34]. Quindi, riassumendo, un'attività d'indagine è considerata «prevista dalla legge» quando ha una base – di creazione legislativa o giurisprudenziale – nel diritto interno, è conoscibile dall'interessato e quest'ultimo deve essere in grado di prevedere le conseguenze derivanti dall'applicazione della misura nei suoi confronti.

Tuttavia, la Corte EDU si è dimostrata riluttante nel richiedere agli Stati una rigorosa dimostrazione della reale necessità dell'interferenza, ritenendo quindi rispettati i requisiti di accessibilità e prevedibilità quando siano predisposti degli effettivi rimedi giudiziali interni alle intrusioni alla *privacy* operate dalle autorità pubbliche. In pratica, i cittadini vedono compensato il mancato esame della ragionevolezza dell'intrusione con il riconoscimento di maggiori garanzie procedurali: nel campo della «prevenzione dei reati» (espressamente previsto all'art. 8 par. 2 CEDU) e delle indagini, dunque, il giudizio di proporzionalità fa fatica ad imporsi quando la compressione della libertà dei singoli risponde all'interesse della giustizia, ove gli interessi alla *privacy* dei singoli cedono più facilmente di fronte alla prerogativa statale dell'esercizio del potere punitivo.

Allo stesso modo, sul criterio della riserva di legge richiesto dall'art. 8 CEDU per stabilire se e come si rende possibile l'ingerenza della pubblica autorità nella propria sfera privata, la stessa Corte ha adottato una nozione ampia di "legge", «ricomprendendovi oltre alla legge in sé anche l'interpretazione che ne dia la giurisprudenza, a condizione però che si tratti di interpretazioni in linea con il testo normativo, coerenti con lo stesso e prevedibili»[35].

BER%22,%22CHAMBER%22],%22itemid%22:[%22001-100293%22]}, consultato da ultimo in data 21 giugno 2022), ove si afferma che «*in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, compatibility with the rule of law requires that domestic law provides adequate protection against arbitrary interference with Article 8 rights. […] The Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law*» (tradotto: «nell'ambito delle misure segrete di sorveglianza adottate da pubbliche autorità, a causa della mancanza di un controllo pubblico e del rischio di abuso di potere, la compatibilità con lo Stato di diritto richiede che la legge nazionale fornisca un'adeguata protezione contro ingerenze arbitrarie nei diritti di cui all'articolo 8. […] La Corte deve convincersi del fatto che esistano garanzie adeguate ed effettive contro gli abusi. Questa valutazione dipende da tutte le circostanze del caso di specie, come la natura, lo scopo e la durata delle possibili misure, i motivi richiesti per ordinarle, le autorità competenti ad autorizzarle, ad eseguirle ed a controllarle, e il genere dei rimedi predisposti dall'ordinamento interno»).

[34] Cfr. Corte EDU, *S. and Marper v. the United Kingdom*, cit., par. 66.

[35] Così, S. SIGNORATO, *Le indagini digitali*, op. cit., p. 260. Per una declinazione di tale impostazione, si veda Corte EDU, *Uzun v. Germany*, cit., par. 62: «*in any system of law, including criminal law, however clearly drafted a legal provision may be, there is an inevitable element of judicial interpretation. There will always be a need for elucidation of doubtful points and for adaptation to changing circumstances. Indeed, in the Convention States, the progressive development of the criminal law through judicial law-making is a well entrenched and necessary part of legal tradition. The Convention cannot be read as outlawing the gradual clarification of the rules of criminal liability through judicial interpretation from case to case, provided that the resultant development is consistent with the essence of the offence and could reasonably be foreseen*» (tradotto: «in ogni sistema giuridico, incluso il diritto penale, per quanto una disposizione legislativa possa essere redatta in modo chiaro, c'è un'inevitabile componente di interpretazione

Inoltre, nel caso *Uzun v. Germany*, nel quale è stata dichiarata compatibile con il sistema di protezione europea dei diritti la sorveglianza di indagati effettuata a mezzo di GPS (*Global Positioning System*) posto su una vettura, la Corte ha creato un doppio binario di identificazione della legge, delineandone un significato "forte" e uno "debole", che potrebbe essere integrato anche da mere prassi[36]. Solo a fronte di indagini caratterizzate da una profonda invasività dei diritti fondamentali, il riferimento va fatto all'accezione "forte" di legge, bastando nei casi di limitazione minore uno scrutinio meno severo[37]: infatti, la Corte «*finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications […], are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations […]. It will therefore apply the more general principles on adequate protection against arbitrary interference with Article 8 rights*»[38] come sopra sintetizzati riferendosi ai principi di prevedibilità e accessibilità[39].

La Corte, in sostanza, riconosce che ci possono essere diversi gradi di limitazione della vita privata, in ragione del tipo di informazioni che si apprendono e del luogo in cui vengono captate, con la conseguenza che la disciplina delle diverse tecnologie di indagine deve essere differenziata quanto a presupposti applicativi e autorità competente ad adottarle. Dunque, in sede di valutazione della lesione dell'art. 8 CEDU, non è possibile fare riferimento ad una scala di valori ferma e omogenea per tutte le attività di intrusione nella sfera privata degli indagati, ma si rende necessario analizzare nello specifico quale mezzo di indagine è stato utilizzato, le modalità d'impiego ed i presupposti applicativi, la necessità che ha portato all'intervento invasivo, la durata della misura e la proporzionalità dell'intrusione rispetto al tipo di reato che si intendeva perseguire.

---

giudiziaria. Ci sarà sempre bisogno di chiarire i punti dubbi e di adattamento alle mutevoli circostanze. Invero, negli Stati parte della Convenzione, il progressivo sviluppo del diritto penale attraverso l'attività creatrice della giurisprudenza è un elemento ben radicato e necessario della tradizione giuridica. La Convenzione non può essere interpretata nel senso di escludere il graduale chiarimento delle norme sulla responsabilità penale attraverso l'interpretazione giurisprudenziale caso per caso, a condizione che l'evoluzione risultante sia coerente con l'essenza del reato e possa essere ragionevolmente prevista»).

[36] Cfr. Corte EDU, *Kruslin c. Francia*, (Serie A n. 176-A), 24 aprile 1990, par. 29.

[37] Nel caso di specie, la Corte EDU osserva che per la sorveglianza effettuata attraverso il rilevatore GPS non risulta necessario applicare lo stesso «*strict scrutiny*» sviluppato dalla sua giurisprudenza in materia di intercettazioni di conversazioni, che trovava la propria base legale nel codice tedesco di procedura penale (anche se lo stesso codice era stato modificato in senso garantista dopo questo caso), e che i gravi reati di cui era accusato il ricorrente giustificavano l'utilizzo di tale misura investigativa, proporzionata rispetto agli scopi perseguiti.

[38] Tradotto: «ritiene questi criteri piuttosto severi, stabiliti e applicati nello specifico contesto della sorveglianza delle telecomunicazioni […], non siano applicabili ai casi come quello di specie, relativo alla sorveglianza via GPS di spostamenti in luoghi pubblici e, quindi, ad una misura che interferisce in misura minore nella vita privata della persona interessata rispetto all'intercettazione delle sue conversazioni telefoniche […]. Saranno quindi applicabili i più generali principi sulla tutela adeguata contro ingerenze arbitrarie nei diritti di cui all'articolo 8». In questi termini, Corte EDU, *Uzun v. Germany*, cit., par. 66.

[39] Principi descritti nel par. 63 citato in nota (v. *supra*).

Tra l'altro, questa impostazione non può che avere delle ricadute sulla valutazione di quando possa ritenersi integrato il requisito della previsione di legge in merito alle indagini digitali di volta in volta eseguite. In ambito interno, per procedere con l'individuazione della corretta qualificazione giuridica dei vari strumenti investigativi a disposizione delle autorità pubbliche, si dovrà, per prima cosa, considerare i diritti fondamentali compressi attraverso gli stessi. In questo modo sarà possibile verificare se tali strumenti di acquisizione probatoria possano rientrare nell'ambito degli istituti tipici di cui agli artt. 244 e ss. c.p.p. e, in caso di esito affermativo, a quali condizioni. In caso di risposta negativa, invece, si apre la possibilità di considerarli mezzi di ricerca della prova atipici, ferma restando la necessità di vagliare la legittimità costituzionale – quale primo limite di ammissibilità di una prova «non disciplinata dalla legge» (art. 189 c.p.p.) – dell'elemento probatorio che si intende assumere: in pratica, l'utilizzabilità di una prova atipica dipende dal rango del diritto inciso.

Se l'atto d'indagine compromette totalmente il nucleo duro di un diritto fondamentale, si dovrà riconoscere un limite costituzionale assoluto, con la conseguenza che l'atto compiuto sarà inutilizzabile (e lo sarà anche per le indagini future, stante anche l'impossibilità di prevedere una normativa espressa contraria ai dettami costituzionali). Allo stesso modo, l'atto che, in assenza di una disposizione normativa, determini una compressione del diritto nel rispetto dei limiti della riserva di legge, del principio di determinatezza della disciplina (che si esplica nei corollari di prevedibilità e accessibilità) e di proporzionalità, sarà inutilizzabile, ma un intervento legislativo potrà disciplinare tale strumento di acquisizione della prova. Invece, nel caso in cui un atto d'indagine leda un diritto emergente, cioè una situazione soggettiva che solitamente viene collocata nella clausola aperta di cui all'art. 2 Cost., che non è protetta da garanzie specifiche, potrà configurarsi una prova atipica rafforzata, da introdursi attraverso un provvedimento debitamente motivato del pubblico ministero. Infine, il dato acquisito riguardante una situazione irrilevante a livello costituzionale sarà utilizzabile anche se l'atto è compiuto dalla polizia giudiziaria nel l'ambito di una attività di indagine atipica[40].

Per quanto riguarda le prove lesive dei diritti emergenti, si pensi, ad esempio, alle videoriprese di immagini non comunicative in luoghi riservati non rientranti nel concetto "forte" di domicilio, per le quali la giurisprudenza ha fatto discendere dall'art. 2 Cost. l'obbligo di un decreto autorizzativo motivato dell'autorità giudiziaria[41]. Invece, tra le prove costituzionalmente indifferenti si possono menzionare le videoriprese di mere immagini in luoghi pubblici, tanto se avvenute al di

[40] Per un'analitica descrizione della griglia di riferimento e dei vari passaggi indicati, si veda G.M. BACCARI – C. CONTI, *La corsa tecnologica*, op. cit. pp. 718-722.

[41] Cfr. Cassazione penale, Sez. un., sentenza n. 26795/2006 (sentenza «Prisco»), pp. 23-24 (sentenza reperibile *online* al collegamento http://servizi.ceda.unina.it/PHP/spec/spec/Cass_26795_2006.pdf, consultato da ultimo in data 21 giugno 2022).

fuori del procedimento, quanto se avvenute nell'ambito delle indagini[42], oppure il pedinamento satellitare mediante GPS[43].

Dunque, la concreta applicabilità dell'art. 189 c.p.p. dipenderà poi dal tipo di diritto fondamentale coinvolto e dall'intensità della limitazione. Esemplificativa è la giurisprudenza in tema di riprese video: le riprese effettuate nel domicilio sono vietate perché lesive dell'art. 14 Cost., mentre quelle che avvengono in "luoghi riservati", tutelati dall'art. 2 Cost., sono legittime, in mancanza di una disciplina *ad hoc*, a condizione che siano autorizzate con decreto motivato dell'autorità giudiziaria: infatti, al di là «di quanto avviene per le registrazioni di comportamenti comunicativi in spazi di privata dimora, che sottostanno alle norme sancite per le intercettazioni, le videoriprese rilevano sotto forma di prova atipica *ex* art. 189 c.p.p., con tre importanti precisazioni: a) costituiscono prova atipica ammissibile se eseguite in luoghi pubblici, aperti al pubblico o esposti al pubblico, anche d'iniziativa della polizia giudiziaria; b) nel caso siano condotte in contesti diversi dal domicilio ove però si innestino profili di riservatezza (cd. luoghi "riservati"), trovano ingresso *ex* art. 189 c.p.p. solo se autorizzate con provvedimento dell'autorità giudiziaria che le giustifichi rispetto alle esigenze investigative e all'invasività dell'atto; c) sono illegittime e processualmente inutilizzabili se filmano condotte non comunicative in luoghi di domicilio, in quanto lesive dell'art. 14 Cost.»[44].

In generale, in mancanza di discipline speciali, il requisito della previsione di legge potrebbe ritenersi integrato sulla base della disciplina degli artt. 55, 189, 326 e 348 c.p.p., nei casi in cui gli atti investigativi si caratterizzino per un'incisività minima alla *privacy*. Tuttavia, la totale mancanza di espresse indicazioni circa le condizioni che legittimano l'autorità pubblica ad adottare una misura investigativa non sembrano integrare il sistema di garanzie enucleato dalla Corte EDU per

[42] Cfr. Cassazione penale, *ult. cit.*, p. 10.

[43] In merito alla tecnica investigativa GPS, la giurisprudenza interna l'ha sempre ritenuta una semplice attività atipica di polizia giudiziaria, che può quindi disporne senza la previa pronuncia di un decreto motivato del pubblico ministero. Tuttavia, se, da un lato, l'interpretazione giurisprudenziale ricadrebbe nella nozione larga di "previsione di legge" per come intesa dalla Corte EDU, fornendo una base legale e rendendo così legittimo l'uso del GPS per finalità investigative, dall'altro, la disciplina italiana risulterebbe totalmente carente sul piano della previsione di chiare garanzie che ne assistano lo svolgimento, ponendo l'atto in chiaro contrasto con la previsione normativa di cui all'art. 8 par. 1 CEDU. Difatti, la stessa Corte EDU nella sentenza *Uzun* cit. ritiene che, in merito al GPS, il diritto alla *privacy* possa sì essere compresso, ma solo a fronte di una normativa *ad hoc* e del provvedimento dell'autorità giudiziaria; questo perché il monitoraggio in tempo reale e costante ottenuto per il suo tramite, pur non essendo paragonabile alla percezione occasionale degli spostamenti di un individuo da parte di terzi passanti occasionali, è caratterizzato da un'invasività minore rispetto alle intercettazioni, che rilevano informazioni sulla condotta, i sentimenti e le opinioni della persona oggetto del controllo. Date queste premesse, S. SIGNORATO, *La localizzazione satellitare*, op. cit., p. 606, giunge alla conclusione per cui «non appare remota la possibilità che l'Italia venga condannata per la violazione dell'art. 8 Cedu, in difetto di idonee garanzie che accompagnino l'uso della localizzazione satellitare, senza considerare che, qualora la tipologia investigativa [GPS] fosse utilizzata per indagini attinenti a reati davvero minimi e/o per periodi particolarmente lunghi, potrebbe venire in rilievo anche un problema di proporzionalità della misura».

[44] In questi termini, M. LANDOLFI, *Le videoriprese investigative tra gli incerti confini giurisprudenziali e le crescenti esigenze di tutela della* privacy, in *Archivio penale*, n. 1/2022, p. 15 (reperibile *online* al collegamento https://archiviopenale.it/File/DownloadArticolo?codice=69c1e8b1-da65-498a-8ffe-c7742508d094&idarticolo=34301, consultato da ultimo in data 21 giugno 2022), commentando la sentenza Cassazione penale, Sez. III., n. 43609/2021.

ammettere una compressione della *privacy*. Solamente l'art. 189, stabilendo che il giudice può ammettere una prova e un mezzo di ricerca della prova atipici, se questi «risulta[no] ideone[i] ad assicurare l'accertamento dei fatti e non pregiudica[no] la libertà morale della persona», e può svolgere un contraddittorio postumo sugli stessi, fornisce delle garanzie, che però non risultano sufficienti a rispondere alle prescrizioni formulate dalla Corte EDU. Stando così le cose, la normativa italiana sembrerebbe convenzionalmente conforme rispetto alle indagini digitali atipiche meno invasive, ma non in rapporto a quelle che determinano significative compressioni dei diritti fondamentali, rendendo necessaria un'attenta valutazione della proporzionalità tra la lesione del diritto rilevante nel caso di specie e le esigenze per le quali si attua la limitazione[45].

Inoltre, la violazione del diritto alla *privacy* e di altri diritti emergenti potrebbe generare un'ulteriore violazione della Convenzione EDU e della Costituzione italiana, quando l'impiego del dato viziato da contrarietà all'art. 8 CEDU con finalità probatorie possa determinare anche una violazione dell'equo processo.

3.2.2 Violazione della *privacy* e conseguenze sul piano del rispetto dell'equo processo.

Data la capacità intrusiva dei nuovi mezzi investigativi, si rende necessario anche riflettere sugli effetti che l'inosservanza dello schema di approccio sopra descritto può avere sull'equità del processo[46]. Tuttavia, in mancanza di una normativa sovranazionale in materia di prova penale[47], che rimane di pertinenza nazionale, non è dato ritrovare un comune sistema di invalidità della prova per il quale, a fronte della predisposizione normativa di uno schema legale dell'atto probatorio, la prova non corrispondente al modello sia destinata alla neutralizzazione e non possa essere ammessa nel processo. La stessa Convenzione EDU, in ambito di equo processo, dedica poco spazio al tema della validità probatoria, limitandosi ad affermare che ogni accusato ha diritto di «disporre del tempo e delle facilitazioni necessarie a preparare la sua difesa» (art. 6, par. 3, lett. b)) e concentrandosi sull'istituto della testimonianza (lett. d)). Dunque, i rischi che un atto d'indagine contrario al diritto di *privacy* possa comunque far entrare nel processo una prova a carico dell'indagato sono forti e attuali.

La Corte EDU si è più volte confrontata con la tematica dei "frutti dell'albero avvelenato",

[45] Cfr. S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 261-262.

[46] In argomento, approfonditamente, cfr. S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., pp. 77 e ss.

[47] Così, Corte EDU, *Svetina v. Slovenia* (ric. n. 38059/13), 22 maggio 2018, par. 42, ove afferma che, «*while Article 6 § 1 guarantees the right to a fair hearing, it does not lay down any rules on the admissibility of evidence as such, since this is primarily a matter for regulation under national law*» (tradotto: «mentre l'art. 6 par. 1 garantisce il diritto a un equo processo, non prevede alcuna disciplina sull'ammissibilità della prova in quanto tale, dato che si tratta principalmente di una materia disciplinata dal diritto nazionale»).

cioè della sorte a cui destinare le prove ottenute attraverso la violazione di un parametro convenzionale[48], ma «ha sempre evitato di stabilire degli automatismi tra violazione "preesistente" e iniquità processuale, riservandosi di valutare, caso per caso, la complessiva equità del procedimento penale in cui sia stato fatto uso della prova viziata»[49]. Sul punto, infatti, la Corte, da un lato, ha ammesso l'ingresso di prove raccolte in violazione di una previsione convenzionale, quando queste – in quanto corroborate da altre più decisive e comunque raccolte legalmente – non siano risultate determinanti nel provare i fatti oggetto di imputazione[50]; dall'altro, ha stabilito come non possa concludersi per una diretta violazione del diritto a un equo processo di cui all'art. 6 CEDU quando l'imputato ha avuto la possibilità nei vari gradi di giudizio interni di contestare l'ammissibilità e l'attendibilità della prova ottenuta in violazione del diritto di *privacy*[51].

Di conseguenza, si può giungere alla conclusione per cui, ad oggi, non vi sono ricadute dirette sul piano processuale a seguito dell'accertata illegittimità di per sé della prova ottenuta attraverso la raccolta di dati digitali in spregio all'art. 8 CEDU[52]. Gli operatori del diritto si trovano quindi nell'impossibilità di avere dei punti fermi in materia, viste la difficoltà di valutare quale sia il grado di incidenza che le informazioni ottenute illegittimamente hanno comunque esercitato sul procedimento decisorio e la possibilità che la Corte applichi in modo ondivago e imprevedibile i summenzionati orientamenti.

A fronte di questo approccio, a domino, un altro limite si può rilevare in merito alle modalità

---

[48] Frutti avvelenati possono aversi non solo per la violazione di norme procedurali, il cui rispetto rientra nel diritto all'equo processo di cui all'art. 6 CEDU, ma anche in caso di contrasto – tra i più rilevanti – agli artt. 2, 3, 8 e 10, rispettivamente, sul diritto alla vita, sul divieto di tortura, sul diritto al rispetto della vita privata e familiare e sul diritto di libertà di espressione.

[49] Così, S. QUATTROCOLO, *Equità del processo penale*, op. cit., p. 113.

[50] Cfr. Corte EDU, *Gäfgen v. Germany* (ric. n. 22978/05), 1° giugno 2010, par. 180, seconda parte (reperibile *online* al collegamento https://hudoc.echr.coe.int/Eng#{%22itemid%22:[%22001-99015%22]}, consultato da ultimo in data 21 giugno 2022), ove si dice che «*[t]he impugned real evidence was not necessary, and was not used to prove him guilty or to determine his sentence. It can thus be said that there was a break in the causal chain leading from the prohibited methods of investigation to the applicant's conviction and sentence in respect of the impugned real evidence*» (tradotto: «la prova impugnata non era necessaria e non fu utilizzata per provare la sua colpevolezza o per determinare la sua condanna. Si può quindi dire che c'è stata un'interruzione della catena causale che ha portato da metodi d'indagine vietati alla condanna del ricorrente e alla sentenza nel rispetto della prova reale impugnata»).

[51] Cfr. Corte EDU, *Kahn v. the UK* (ric. n. 35394/97), 12 maggio 2000, par. 38 (reperibile *online* al collegamento https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-58841%22]}, consultato da ultimo in data 21 giugno 2022), secondo la quale «*the applicant had ample opportunity to challenge both the authenticity and the use of the recording. He did not challenge its authenticity, but challenged its use at the* voir dire *and again before the Court of Appeal and the House of Lords*» (tradotto: «il ricorrente ha avuto ampie opportunità di contestare sia l'autenticità che l'uso della registrazione. Non ne ha contestato l'autenticità, ma ne ha contestato l'uso al *voir dire* e ancora davanti alla Corte d'Appello e alla Camera dei Lords»).

[52] Cfr., Corte EDU, *Svetina v. Slovenia*, cit., par. 48, che afferma: «*The Court notes in this connection that it has already found in several cases where investigative measures interfering with Article 8 rights were not "in accordance with the law" that the admission in evidence of information obtained thereby did not, in the circumstances of the cases, conflict with the requirements of fairness guaranteed by Article 6 § 1. […] The decisive question is whether the proceedings as a whole were fair*» (tradotto: «La Corte rileva al riguardo di aver già riscontrato in diversi casi in cui gli atti investigativi lesivi dei diritti di cui all'articolo 8 non erano "conformi alla legge" che l'ammissione come prova di informazioni così ottenute non è, nelle circostanze dei casi, confliggente con i requisiti di equità garantiti dall'articolo 6 § 1. […] La questione decisiva è se il procedimento nel suo insieme fosse equo»).

di formazione del dato probatorio fornito da dispositivi informatici di cui sia ignoto il funzionamento: infatti, «certi vizi della "*digital evidence*" non riguardano soltanto i dati ottenuti attraverso l'intrusione occulta nella immateriale area della privatezza degli individui, ma caratterizzano tutti gli elementi conoscitivi che derivino dal procedimento automatizzato, nel quale la fonte della conoscenza che si introduce nel processo non è umana, ma è un algoritmo, o un modello, nel cui funzionamento l'apporto umano si riconosce soltanto in fase di design e non di produzione del dato conoscitivo»[53].

Eppure, se le regole procedurali non sono rispettate, se ne dovrebbe dedurre che la prova acquisita non possa dirsi rispettosa di quel criterio minimo di affidabilità stabilito dal legislatore e quindi ammissibile a processo. In tal senso, per l'ambito interno, si potrebbe scorgere una simile *intentio legis* nell'art. 191 c.p.p., per cui la prova acquisita in violazione dei divieti stabiliti dalla legge non può essere utilizzata; tale statuizione, però, non potrebbe farsi valere in via analogica nel caso *de qua*, cioè nel tentativo di trovare un espresso riferimento normativo che determini l'automatica inutilizzabilità delle prove acquisite in violazione di una norma procedurale o di un determinato diritto: infatti, l'art. 191 c.p.p. si riferisce alle prove acquisite in violazione dei divieti stabiliti dalla legge e non a quelle la cui assunzione, pur consentita, sia avvenuta senza l'osservanza delle formalità prescritte. Si potrà valutare se si versi in uno dei casi di nullità previsti dal codice di procedura penale.

Per chiarire il generale orientamento giurisprudenziale sul fatto di far derivare o meno l'inutilizzabilità della prova acquisita illegalmente, la stessa Corte costituzionale[54], in merito allo specifico rapporto tra perquisizione e sequestro, ha fatto comunque trasparire apertura circa la propagazione dell'invalidità dell'atto d'indagine alla fonte di prova così appresa (viziando gli elementi di prova dallo stesso eventualmente ottenuti), facendo riferimento all'art. 185, co. 1 c.p.p., a norma del quale «la nullità di un atto rende invalidi gli atti consecutivi che dipendono da quello dichiarato nullo». Tuttavia, è ugualmente sempre giunta ad affermare inammissibili le questioni di legittimità costituzionale dell'art. 191 c.p.p., nella parte in cui non prevede che l'inutilizzabilità riguardi anche gli esiti probatori degli atti d'indagine compiuti dalla polizia giudiziaria fuori dei casi tassativamente previsti dalla legge o comunque non convalidati dall'autorità giudiziaria con provvedimento motivato. Nel fare ciò, ha quindi tenuto ferme le conclusioni della Cassazione, la quale aveva affermato che, «se è vero che l'illegittimità della ricerca della prova del commesso reato, allorquando assume le dimensioni conseguenti ad una palese violazione delle norme poste a tutela dei diritti soggettivi oggetto di specifica tutela da parte della Costituzione, non può, in linea generale, non diffondere i suoi effetti invalidanti sui risultati che quella ricerca ha consentito di

[53] Così, S. QUATTROCOLO, *Equità del processo penale*, op. cit., p. 115.
[54] Cfr., *ex multis*, Corte costituzionale, sentenze nn. 219/2019 e 252/2020.

acquisire, è altrettanto vero che allorquando quella ricerca, comunque effettuata, si sia conclusa con il rinvenimento ed il sequestro del corpo del reato o delle cose pertinenti al reato, è lo stesso ordinamento processuale a considerare del tutto irrilevante il modo con il quale a quel sequestro si sia pervenuti»[55].

Dunque, se il brocardo latino "*male captum bene retentum*" (da rendersi come il principio secondo il quale, sebbene acquisita illegalmente, la prova è utilizzabile) si fa largo per i mezzi tipici della ricerca della prova, a maggiore ragione si rende necessario riflettere sull'ammissibilità della prova ottenuta per il tramite di mezzi atipici di investigazione, categoria, appunto, nella quale rientrano facilmente (quasi) tutti i nuovi strumenti d'indagine utilizzati in ambito investigativo. Allo stato, infatti, la raccolta della prova avvenuta contrariamente ai limiti legislativi viene perseguita dall'ordinamento con la sanzione in sede disciplinare e penale dell'agente autore della condotta abusiva e nulla è detto sull'inutilizzabilità processuale della prova ottenuta con l'attività d'indagine non rispettosa dei parametri legislativi.

Come è stato osservato specificamente in tema di algoritmo di polizia predittiva[56], «il rispetto della normativa *extra codicem* in tema di *privacy* nulla dice circa l'attendibilità e l'utilizzabilità nel processo penale della prova raccolta mediante algoritmi di intelligenza artificiale»[57]. Da un lato, «dal punto vista processuale l'inutilizzabilità della prova dipende unicamente dalla violazione di un divieto probatorio, sia esso espresso o tacito»[58]: infatti, «la validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali» (art. 160-*bis* Codice Privacy). Dall'altro, «*a contrario* si può sostenere che il formale rispetto della normativa *privacy* è auspicabile ma non dirimente ai fini della *spendibilità* processuale della prova raccolta mediante algoritmi di intelligenza artificiale. È infatti alle disposizioni del codice di rito che bisogna guardare per determinare quanto la prova scientifica di natura informatica basata su algoritmi di intelligenza artificiale sia utilizzabile e attendibile per la ricostruzione e l'accertamento dei fatti»[59].

Dunque, la stessa Corte EDU, in mancanza di una regola generale di esclusione probatoria dei "frutti dell'albero avvelenato", «tende a convogliare tutte le valutazioni sull'ammissibilità e

[55] Così, Cassazione penale, Sez. un., sentenza 27 marzo 1996 (sentenza «Sala»).

[56] La questione nasce dal fatto che l'algoritmo SARI Real Time, attraverso il quale si rende possibile l'attività di riconoscimento facciale in modalità dinamica, esegue una modalità di trattamento dati biometrici non previsto dalla normativa vigente. Proprio per questo motivo, il Garante Privacy – con parere n. 127/2021 cit. – ha affermato che SARI Real Time non è conforme alla normativa sulla *privacy*. Le criticità potrebbero essere risolte con l'introduzione di una normativa di settore, ai sensi dell'art. 7 D.Lgs. 51/2018, eventualmente anche di natura regolamentare, secondo quanto previsto dall'art. 5, co. 2 D.Lgs. 51/2018.

[57] In questi termini, M. TORRE, *Nuove tecnologie e trattamento dei dati*, op. cit., p. 1052.

[58] *Idem*, p. 1052.

[59] *Idem*, p. 1052.

sulla utilizzabilità della prova in un generale test di compatibilità con il processo equo, inteso come nozione onnicomprensiva che calibra e combina le singole garanzie di dettaglio»[60]. Tra queste garanzie volte a garantire l'equità complessiva del processo, vi sono i principi del contraddittorio nella formazione della prova e della parità delle armi. L'ammissione e la valutazione di prove generate automaticamente, però, rischia di creare un *vulnus* a tale sistema, in quanto le stesse sembrano caratterizzarsi per un'autosufficienza indiscutibile che renderebbe superfluo ogni confronto sulla loro affidabilità e sul modo in cui sono state generate e assunte. Si tratta di un rischio inaccettabile nel sistema delle garanzie del giusto processo, che vuole tutte le parti, giudice compreso, nelle condizioni di poter aver pieno accesso alle modalità di formazione della prova[61].

3.3 La prova digitale e i rischi per la parità delle armi.

L'impiego processuale di dati ed elementi conoscitivi generati automaticamente da algoritmi, a prescindere che siano stati o meno creati per essere impiegati all'interno di un procedimento, ha un forte impatto sul sistema penale anche sotto il profilo della parità delle armi tra le parti. Ci si deve domandare, infatti, se è possibile contestare l'attendibilità e l'accuratezza del dato, generato e/o raccolto per mezzo di un algoritmo.

Generalmente, in ambito penale, la parità delle armi non determina la necessaria identità di posizioni tra le parti o di facoltà di cui avvalersi[62], ma si traduce nella possibilità di presentare le proprie argomentazioni in condizioni paritarie all'altra parte. Ciò si realizza, in concreto, riconoscendo alle parti i diritti di avere effettiva conoscenza delle allegazioni e delle argomentazioni della controparte e di poterle contestare in contraddittorio di fronte a giudice terzo e imparziale (art. 111, cc. 2-4 Cost.).

Tuttavia, quando ci si trova a valutare l'affidabilità del dato generato da un *software*, si ergono degli ostacoli relativi alla natura e alla genesi dello stesso. Infatti, soltanto attraverso l'accessibilità e la trasparenza dell'algoritmo è possibile valutare e, se del caso, contestare il risultato della sua elaborazione. Non a caso, le stesse Carte etiche sopra analizzate spingono per il riconoscimento del nuovo diritto alla intelligibilità del sistema informatico e alla sua comprensione.

Il concetto di trasparenza necessita di essere tradotto in misure concrete, le quali, però, incontrano a loro volta degli ostacoli. Infatti, la rivelazione del codice sorgente alla base degli

[60] Così, S. QUATTROCOLO, *Processo penale e rivoluzione digitale*, op. cit., p. 128.
[61] Cfr. A. ZIROLDI, *Intelligenza artificiale e processo penale*, op. cit., p. 10.
[62] Ad esempio, se nella fase delle indagini preliminari fossero previste delle condizioni paritarie tra pubblico ministero e indagato, le indagini stesse sarebbero inefficaci e non consentirebbero la scoperta delle prove e individuazione dell'autore del reato.

algoritmi, come già visto, si scontra con l'interesse dell'autorità inquirente di non svelare le modalità di funzionamento degli strumenti con i quali sono state svolte le indagini (la segretezza è il primo elemento che determina l'efficacia soprattutto dei mezzi di captazione) e con la volontà dell'azienda produttrice di mantenere il segreto industriale derivante dal diritto di proprietà intellettuale sul codice stesso. A ciò si può aggiungere il fatto che l'algoritmo possa non essere stato progettato secondo criteri di trasparenza e responsabilizzazione, tali da rendere comprensibili e verificabili i risultati dell'elaborazione a chi non sia il progettista del codice sorgente.

Tra l'altro, l'accesso al codice sorgente può non essere comunque sufficiente a giustificare e a spiegare i risultati ottenuti da meccanismi di autoapprendimento, rendendo quindi necessario predisporre dei protocolli volti a permettere il controllo *ex post* del funzionamento dell'intelligenza artificiale. Tuttavia, l'intellegibilità del sistema non è garantita nemmeno attraverso un controllo successivo all'elaborazione, quando il dispositivo oggetto di verifica si basa su un formato avanzato di autoapprendimento.

Tale fenomeno di asimmetria conoscitiva "digitale" si inserisce nel generale e già noto squilibrio che si riscontra nel processo penale da quando hanno fatto il loro ingresso i saperi tecnici, scientifici e artistici per la soluzione dei casi più difficili e pone problemi concreti nell'attuazione in senso lato del principio della parità delle armi; la parte pubblica può, infatti, usufruire della scienza e delle tecnologie presumibilmente migliori, non dovendo fare i conti, come invece la parte privata, con problemi di ristrettezza economica. «La prova algoritmica, tuttavia, introduce la forma più estrema di tale squilibrio, poiché il risultato probatorio può essere non criticabile laddove, appunto, l'inaccessibilità del codice sorgente o altre caratteristiche del *software* non consentano alla parte contro la quale la prova è introdotta nel processo di contestarne l'accuratezza e l'attendibilità»[63]. La difesa, quindi, non si trova nella piena possibilità di respingere in modo convincente la presunta attendibilità della prova digitale, che, per il fatto di essere il prodotto (ritenuto dalla società intrinsecamente affidabile) di una macchina, si afferma di per sé. Allo stesso tempo, a causa della mancata contestazione della prova digitale, il giudice finirebbe più facilmente per assumere un atteggiamento di passiva e acritica accettazione circa la sua intrinseca affidabilità.

La possibilità di accedere al codice sorgente è, quindi, cruciale sotto il profilo della controllabilità dell'algoritmo; diversamente, nascerebbero le condizioni per la creazione di buchi neri giuridici (*legal black hole*), con il conseguente imporsi di decisioni assimilabili a quelle prive di motivazioni, con motivazione meramente apparente o, addirittura, segrete, in assoluto contrasto con gli artt. 24, co. 2 e 111, co. 6 Cost. (sul diritto di difesa e sulla necessità della motivazione per i provvedimenti giurisdizionali) e con l'art. 13 CEDU (sul diritto a un ricorso effettivo).

[63] Ne è convinta S. QUATTROCOLO, *Equità del processo penale*, op. cit., p. 118.

Inoltre, sotto il profilo dell'affidabilità dell'algoritmo, l'accuratezza del dato risultante dell'elaborazione computazionale «dovrebbe essere fatta oggetto di valutazione peritale – non diversamente da ogni acquisizione scientifica che entri nel processo penale –, e comunque essere discussa in contraddittorio nella sua fondatezza empirica, a pena di una evidente violazione […] del diritto di difesa»[64].

Dunque, anche prescindendo dall'esistenza di una violazione del diritto alla *privacy* commessa con un atto d'indagine illecito o sproporzionato, l'impossibilità o l'estrema difficoltà di accedere al codice sorgente per comprendere a monte il funzionamento del dispositivo informatico o di poter effettuare un controllo in una fase successiva sui dati generati e/o raccolti per mezzo dello stesso rischia di tradursi in una violazione del parametro convenzionale di cui all'art. 6, par. 1 CEDU, specie ove afferma che ogni persona ha diritto di vedere il suo caso trattato da un tribunale in grado di «pronunciarsi» – quindi, di comprendere e valutare – «sulla fondatezza di ogni accusa penale formulata nei suoi confronti».

Questa asserzione di principio, però, non sarebbe in grado da sola di portare la Corte EDU a pronunciarsi per una violazione dell'equo processo, visto il suo orientamento favorevole a valutare l'equità del procedimento nel suo complesso e non solo limitatamente a determinate questioni. Alcuni principi e strumenti tecnici e processuali potrebbero, infatti, permettere alla difesa (e, allo stesso modo, alla parte pubblica) di confutare la validità della prova digitale utilizzata dalla controparte e metterla così in condizione di esercitare pienamente il diritto di difesa.

Anzitutto, sul versante meramente tecnico, sono stati realizzati degli algoritmi di crittografia, basati sui modelli della c.d. "dimostrazione a conoscenza zero" (*zero-knowledge proof*), in grado di dimostrare che un'affermazione (solitamente matematica) è vera, senza rivelare nient'altro oltre alla veridicità della stessa. Attraverso questi strumenti, quindi, la difesa potrebbe «*challenge the accuracy of inculpatory evidence without implying, necessarily, the disclosure of the codes and, therefore, the rewriting of them*»[65]. si potrebbe determinare l'accuratezza del dato in uscita senza che sia necessario rendere noto il codice sorgente o il funzionamento dell'algoritmo.

Il rischio che l'algoritmo di crittografia utilizzato possa essere a sua volta messo in discussione dalla parte che si vede contestata la prova a favore, innescando così uno scontro sugli strumenti utilizzati per confutarla, rientrerebbe nella normale dialettica che si viene a creare tra consulenti tecnici delle parti opposte sulla bontà delle rispettive tecniche utilizzate. Anche se

[64] Così, V. MANES, *L'oracolo algoritmico e la giustizia penale*, op. cit., p. 16.

[65] Tradotto: «contestare l'esattezza delle prove a carico senza che ciò implichi, necessariamente, la divulgazione dei codici e, quindi, la loro riscrittura». In questi termini, S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., p. 95. L'Autrice ha infatti evidenziato come l'accesso ai codici sorgente degli strumenti investigativi implicherebbe la necessità di sostituire/riscrivere costantemente tali codici per evitare che il crimine, venutone a conoscenza, possa prendere immediate e generali contromisure *pro futuro* (cfr. p. 92).

l'utilizzo di tale strumento algoritmico non risolverebbe alla radice e in modo univoco la questione sulla bontà o meno del dato prodotto dal dispositivo di cui si tratta, il giudice tornerebbe almeno nella posizione di poter vagliare diverse spiegazioni scientifiche e così verificare la correttezza dei metodi con le quali sono state portate alla sua attenzione, come avviene in tutti i processi nei quali trova ingresso la prova tecnologica e scientifica "tradizionale", cioè non digitale[66]. D'altra parte, però, in tale situazione (come in sede di perizia) il giudice si ritroverebbe a dover giudicare su questioni specialistiche delle quali non può avere diretta e approfondita conoscenza. Ad ogni modo, l'impiego nel processo di tali algoritmi certificatori, riuscendo a spiegare il funzionamento del dispositivo evitando l'ostacolo del segreto industriale posto a protezione del codice sorgente, potrebbe risultare sufficiente a garantire la parità delle armi.

Un altro modo per permettere alla difesa di argomentare sulla validità della prova potrebbe essere quello di rendere disponibili le specifiche tecniche che illustrano il funzionamento dell'algoritmo che l'ha generata. Come detto, tale soluzione non sarebbe praticabile con riguardo agli strumenti di captazione, ma lo potrebbe essere con quegli strumenti di polizia predittiva che svolgono funzioni in ambito preventivo e le cui elaborazioni, solo in determinati casi, possono avere delle conseguenze dirette in ambito procedimentale (su tutti, i dispositivi di polizia predittiva che, nella ricerca del collegamento criminale, si avvalgono anche delle riprese video). Nel momento in cui si propende per un auspicato intervento di tecnici e studiosi in sede di validazione di tali strumenti di polizia predittiva, la predisposizione di un libretto tecnico che ne spiegasse il funzionamento e fosse fruibile dagli interessati ne sarebbe una logica conseguenza[67].

Al di là dell'ipotesi di verificare strumenti i cui codici sorgenti siano aperti, le parti processuali avranno a che fare più probabilmente con sistemi non trasparenti: di conseguenza, «la valutazione dell'attendibilità della prova algoritmica non potrà aver luogo che attraverso lo strumento peritale, che costituisce la sola soluzione attualmente compatibile con il quadro dei principi processuali e delle garanzie del *fair trial*»[68].

Il giudice, infatti, potrebbe dover fare ricorso alla perizia (artt. 220 e ss. c.p.p.) per verificare l'attendibilità della prova digitale. Attraverso la nomina di un perito, otterrebbe una certificazione indipendente sul funzionamento dell'algoritmo che ha generato la prova oggetto di contestazione e sulla validità o meno *ex post* dei risultati frutto dell'elaborazione; certificazione che le parti in contrapposizione nel processo, specialmente la difesa, potrebbero successivamente utilizzare per

[66] L'argomentazione andrebbe svolta sempre secondo i criteri Daubert, già enunciati in Capitolo III, nota n. 9.

[67] Tale soluzione, a dire il vero, sarebbe più adeguata nei confronti di strumenti di giustizia predittiva con funzioni di ausilio per il giudice. Nel caso *Loomis*, infatti, la Corte rigettò la contestazione della difesa in merito alla non accessibilità del dispositivo COMPAS valorizzando il fatto che la società produttrice, pur non svelando il codice sorgente, aveva messo a disposizione il relativo libretto di istruzioni.

[68] Propende per tale conclusione A. ZIROLDI, *Intelligenza artificiale e processo penale*, op. cit., p. 11.

argomentare sull'inaffidabilità o inaccuratezza dei dati, quindi della prova.

In sede di perizia, tuttavia, la difesa potrebbe propendere per la nomina di un proprio consulente tecnico *ex* art. 225, co. 1 c.p.p. e ciò solleva, nuovamente, la problematica del segreto industriale. Come è stato notato, «i consulenti di parte dovrebbero essere immessi nella conoscenza degli stessi elementi forniti al perito, per consentire loro di svolgere il proprio incarico; tuttavia non pare sussistere, sul piano processuale, un divieto di divulgazione, da parte del professionista nominato dalla difesa, degli elementi appresi durante tale ufficio […]. Trattandosi, infatti, di attività probatoria dibattimentale, non paiono sussistere limiti formali processuali all'eventuale divulgazione di quanto appreso»[69]. A ben vedere, nell'ordinamento già si ritrovano delle norme rivolte a consulenti tecnici e periti ausiliari sul trattamento dei dati personali di cui vengono a conoscenza nell'espletamento delle relative incombenze: infatti, la delibera n. 46/2008 del Garante Privacy stabilisce che il consulente e il perito «possono trattare lecitamente dati personali, nei limiti in cui ciò è necessario per il corretto adempimento dell'incarico ricevuto e solo nell'ambito dell'accertamento demandato dall'autorità giudiziaria»[70]. Su tale scia, sarebbe quindi possibile e auspicabile un intervento *ad hoc* del legislatore volto a trovare un bilanciamento tra il segreto industriale e le esigenze di giustizia e, nei casi in cui propenda per le seconde, imporre a consulenti e periti dei rigidi obblighi di trattamento dei dati tecnici e commerciali acquisiti sul funzionamento degli algoritmi informatici oggetto di confronto. A presidio dell'eventuale violazione di tali obblighi, si potrebbe fare riferimento alla sanzione penale di cui all'art. 379-*bis* c.p., che potrebbe essere integrata con la previsione di una sanzione speciale e più grave in caso di rivelazione dei dati indicati (visti gli interessi economici delle aziende in gioco, già in parte sacrificati a monte nell'eventualità in cui fosse imposto l'accesso ai codici per le esigenze di giustizia).

Inoltre, anche in tal sede si riproporrebbe lo scontro tra consulenti poco prima menzionato, con la conseguenza per il giudice di dover prendere una decisione su materie tecniche a lui estranee, vestendo i panni di una sorta di *peritus peritorum* per ergersi ad arbitro in tale disputa[71]. Quanto

[69] Così, S. QUATTROCOLO, *Equità del processo penale*, op. cit., p. 122. Soprattutto la figura del consulente tecnico del pubblico ministero viene, nell'orientamento giurisprudenziale, equiparata al testimone. In tal senso, cfr. Cassazione penale, Sez. un., ordinanza n. 43384 del 27 giugno 2013 e Corte costituzionale, sentenza n. 163/2014, secondo la quale la «parificazione del consulente tecnico al testimone troverebbe, in effetti, un solido appiglio ermeneutico nell'art. 501 cod. proc. pen., che estende al consulente tecnico le disposizioni sull'esame dibattimentale dei testimoni. Pur non essendo un testimone in senso proprio – in quanto non chiamato a riferire su «fatti», ma ad esprimere valutazioni su materie che richiedono specifiche competenze – il consulente tecnico ben potrebbe, d'altra parte, «affermare il falso o negare il vero», conformemente alla previsione dell'art. 372 cod. pen., o «rendere dichiarazioni false», secondo quella dell'art. 371-bis cod. pen., ad esempio tacendo o alterando determinati esiti obiettivi degli accertamenti espletati, ferma restando l'esclusione di «ogni sindacato sugli aspetti meramente valutativi relativi a detti accertamenti»».

[70] In questi termini, Garante Privacy, Delibera n. 46/2008, par. 2.2 (reperibile *online* al collegamento https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1534086, consultato da ultimo in data 21 giugno 2022).

[71] La Cassazione, tra l'altro, ha statuito che al giudice è inibito disattendere i risultati di una perizia di parte sulla sola base della propria scienza personale. Nel caso in cui non condivida le conclusioni del consulente tecnico di parte e

meno, però, in tale scenario il confronto sarebbe incentrato direttamente sul codice sorgente dell'algoritmo che ha generato la prova e non sullo strumento di crittografia digitale che, in via mediata, ha validato o meno il funzionamento del dispositivo senza nulla dire sul codice stesso, avvicinando le parti a discutere del nocciolo della questione.

Dunque, l'insieme dei rimedi appena presentato non riesce a risolvere in modo definitivo – né a monte, né a valle – il problema dell'accesso nel processo penale di prove generate automaticamente. Ogni apparente soluzione porta con sé degli inconvenienti, ma, in assenza di qualsiasi accorgimento, sarebbe impossibile evitare la violazione del principio dell'equo processo.

Sulla scia delle Carte etiche volte all'affermazione di un'IA trasparente (*explainable AI*), almeno per quanto riguarda gli algoritmi di polizia predittiva, una soluzione risolutiva potrebbe essere quella di rendere noto il codice sorgente, far riconoscere a terzi esperti l'affidabilità del funzionamento dell'algoritmo e pubblicare le relative specifiche tecniche. Tale possibilità, però, sembra configurarsi come un'eccezione, in quanto gli strumenti investigativi di captazione si prestano maggiormente, per loro funzione, ad essere oggetto di secretazione circa la loro costituzione e il loro funzionamento.

Per superare gli ostacoli detti, intervenendo a livello normativo procedurale, si potrebbero prevedere delle norme volte a ottenere una divulgazione protetta del codice sorgente che mettano in equilibrio tra loro gli interessi alla segretezza del proprietario del *software* con il principio di pubblicità del giudizio; oppure, prendendo spunto dagli istituti della perizia e del consulente tecnico del p.m. (art. 359 c.p.p.), elaborare una regola che, solo negli specifici casi nei quali è sollevato un problema di opacità algoritmica (quindi, una *lex specialis*), imponga al proprietario dell'algoritmo – il quale, dunque, non può rifiutare la sua opera – di fornire la sua consulenza al giudice e, in subordine e in modo strettamente necessario, alle parti.

Infine, visto l'orientamento della Corte EDU riguardo all'art. 6, par. 1 della Convenzione, nel caso in cui, sia praticabile sia per la fase *ex ante* che per quella *ex post*, nessuna delle soluzioni indicate, «la via pare segnata verso l'esclusione dell'ammissione o dell'utilizzazione della [prova], sulla scorta della incompatibilità con l'essenza irrinunciabile del processo equo»[72].

---

sia necessario svolgere un'indagine che presupponga particolari cognizioni scientifiche, deve necessariamente disporre una nuova perizia per risolvere i dubbi e i punti critici. Cfr. Cassazione penale, Sez. III, sentenza n. 12026/2020.

[72] In questi termini, S. QUATTROCOLO, *Processo penale e rivoluzione digitale*, op. cit., p. 132.

3.4 Sull'utilizzabilità processuale dei risultati investigativi ottenuti mediante sistemi automatici.

Ammesso che siano superabili le difficoltà di trovare uno o più metodi per garantire lo svolgimento di un processo equo di fronte alle prove elaborate dai dispositivi informatici, il passo successivo è quello di ricondurre le tipologie investigative svolte attraverso di loro alla categoria dei mezzi di ricerca della prova tipici o atipici. Se, in alcuni casi, l'intelligenza artificiale integra le modalità dei mezzi tipici di ricerca della prova, in altri casi, lo strumento ha caratteristiche tali da renderlo non riconducibile ad uno dei modelli previsti dal legislatore, rendendo difficile e incerta la verifica di quale sia la disciplina da considerare.

In generale, i mezzi di ricerca della prova informatici si caratterizzano per il fatto di ledere maggiormente i diritti fondamentali rispetto ai tradizionali metodi investigativi. Di conseguenza, nella ricostruzione della normativa applicabile ai singoli atti d'indagine informatica sarà necessario procedere di pari passo con l'individuazione di tutele adeguate, considerato che, a maggior ragione, «una volta ammesso l'impiego di un atto d'indagine, nella prassi è assai frequente che si tenda a dilatarne la sfera applicativa sia sul piano repressivo che preventivo»[73].

Dunque, nella ricerca di una normativa esistente a cui agganciare l'attività d'indagine consentita dal nuovo dispositivo informatico, bisogna salvaguardare la legalità del sistema probatorio, evitando di qualificare come mezzi di ricerca della prova tipici attività investigative che, di fatto, ne forzerebbero i limiti. Come visto, dall'individuazione o meno del carattere fondamentale dei diritti incisi, deriva tutta una serie di considerazioni e/o attività per valutare l'ammissibilità dello strumento d'indagine e stabilire le condizioni per l'assunzione della prova acquisita per suo tramite. Tra l'altro, la scelta di far rientrare l'atto d'indagine nella categoria dell'atipicità deve farsi solo nel momento in cui sia certo che, in tal modo, non si realizzi un'elusione delle regole stabilite dalla legge processuale per un atto tipico, a cui, in realtà, l'atto andrebbe riferito[74].

Se, dall'esame dei diritti fondamentali coinvolti, non risulta possibile inquadrare lo strumento informatico di acquisizione probatoria nell'ambito di istituti tipici, si deve valutare la sua ricaduta tra i mezzi di ricerca della prova atipici, non dimenticando che il limite all'ammissibilità di una prova atipica, cioè «non disciplinata dalla legge» (art. 189 c.p.p.), è la sua legittimità costituzionale. La stessa Cassazione, in tema di operatività del principio di atipicità rispetto a strumenti probatori che incidono su beni costituzionalmente tutelati, non ha mancato di evidenziare come «l'art. 189 c.p.p. […] presuppone la formazione lecita della prova e soltanto in questo caso la rende ammissibile», in quanto «non può considerarsi "non disciplinata dalla legge" la prova basata

[73] Così, S. SIGNORATO, *Le indagini digitali*, op. cit., p. 206.
[74] Cfr. G.M. BACCARI – C. CONTI, *La corsa tecnologica*, op. cit. pp. 719-720.

su un'attività che la legge vieta»[75]. Ad ogni modo, la concreta applicabilità di tale disciplina sarà determinata dal tipo di diritto fondamentale coinvolto e dall'intensità della limitazione.

Nonostante la possibilità di sfruttare la disciplina della prova atipica per acquisire nel processo gli elementi raccolti o elaborati dai dispositivi informatici, la ricostruzione della disciplina giuridica applicabile all'atto non può che essere fatta caso per caso, vista anche la capacità di uno stesso strumento di svolgere diverse funzioni. A titolo esemplificativo di quanto detto, merita di essere riportato il chiaro inquadramento giuridico effettuato in merito alle poliedriche finalità a cui si possono indirizzare i dispositivi di polizia predittiva che utilizzano il riconoscimento facciale: infatti, ove «il riconoscimento abbia una finalità di mera *identificazione*, esso rientrerà nei poteri coercitivi della polizia (art. 4, Testo Unico delle leggi di pubblica sicurezza) oppure nelle prerogative investigative della polizia giudiziaria (art. 349 c.p.p.), a seconda che l'attività venga svolta, rispettivamente, per fini di pubblica sicurezza o per finalità processuali: *nulla quaestio*.

Il sistema automatico di riconoscimento immagini, tuttavia, sembra in grado di poter svolgere anche funzioni diverse, giuridicamente sussumibili nel *genus* dell'*individuazione* (art. 361 c.p.p.) o della *ricognizione* di persone (artt. 213 ss. c.p.p.), a seconda che l'attività di riconoscimento abbia rispettivamente una funzione *investigativa* o *probatoria*. In entrambi questi casi, siamo di fronte a prove atipiche, poiché il riconoscitore non è un uomo ma una macchina. Ciò non pone problemi a patto che il mezzo di prova o il mezzo di ricerca della prova atipico rispetti i seguenti requisiti: idoneità ad assicurare l'accertamento dei fatti; tutela della libertà morale della persona (art. 189 c.p.p.)»[76].

Anche se, formalmente, l'art. 189 c.p.p. si riferisce alle prove atipiche, categoria prevista dal legislatore per non precludere ai soggetti impegnati nella prevenzione e repressione dei reati di fare uso dei progressi scientifici per ricavare elementi di prova non previsti, oggi l'orientamento maggioritario è favorevole all'estensione di tale disciplina agli atti investigativi atipici. Proprio in ragione dell'operatività anche nella fase delle indagini preliminari della norma in questione, l'ammissibilità di tali strumenti investigativi non viene esclusa di per sé a causa della mancanza di una disciplina *ad hoc.*

Secondo l'orientamento contrario, l'art. 189 c.p.p. sarebbe riferibile solo alle prove perché, nel momento in cui stabilisce che «il giudice provvede all'immissione [della prova], sentite le parti sulle modalità di assunzione della [stessa]», per prima cosa, l'espressione "assunzione" può rilevare solo in confronto alle prove e, in secondo luogo, il riferimento ad un contraddittorio anticipato *sulla* prova è realizzabile solo in merito a prove in formazione e non a prove precostituite o a mezzi di

[75] Così, Cassazione penale, Sez. un., sentenza «Prisco» cit., p. 19.

[76] Procede così all'inquadramento giuridico M. TORRE, *Nuove tecnologie e trattamento dei dati personali*, op. cit., pp. 1052-1053.

ricerca della prova atipici[77].

Il fatto che un confronto anticipato sia impossibile in merito alle attività d'indagine ha portato altri a ritenere applicabile l'art. 189 c.p.p. agli atti d'indagine atipici solo in relazione alla necessità che lo strumento informatico utilizzato «risult[i] idone[o] ad assicurare l'accertamento dei fatti e non pregiudich[i] la libertà morale della persona». Dunque, non dovendosi svolgere il contraddittorio, la prova sarebbe ottenuta «senza le garanzie legali dell'art. 189 c.p.p., a meno che non si condivida l'interpretazione di chi vede in quella norma la predisposizione dialettica per l'ammissione della prova, non anche la disposizione garantista per la formazione della prova non prevista dalla legge, che [si reputa] essere il valore effettivo della disposizione»[78]. Se non fosse previsto alcun confronto, si ritiene che si venga a realizzare una chiara violazione dei criteri previsti dalla norma. Allo stesso modo, se si ritenesse comunque possibile realizzare un confronto, questo sarebbe limitato, in realtà, ad un confronto sull'utilizzabilità della prova e nulla direbbe sulla legittimità dell'acquisizione, che sarebbe invece il vero nodo del contendere.

Invece, chi parteggia per la riferibilità dell'art. 189 c.p.p. anche agli atti investigativi sottolinea vari elementi a favore. Anzitutto, rileva la collazione della norma nelle disposizioni generali del Libro terzo del codice di rito: infatti, come indicato dalla *Relazione al Progetto preliminare del codice di procedura penale*, queste potrebbero trovare applicazione anche in riferimento alle attività d'indagine qualora la «struttura delle singole disposizioni» lo consenta[79]. Specificamente, tale requisito sembra esserci, se si considerano le garanzie richieste dalla norma per ammettere prove atipiche dell'idoneità ad assicurare l'accertamento dei fatti e, sulla scia dell'art. 188 c.p.p., non pregiudicare la libertà morale della persona.

In secondo luogo, nella stessa *Relazione al Progetto* l'intenzione del legislatore di garantire al sistema procedimentale una giusta flessibilità di fronte all'innovazione scientifica e tecnologica si riscontra non solo in riferimento alle prove atipiche, ma anche ai mezzi di ricerca della prova atipici: infatti, allo stesso legislatore è «sembrato che una norma così articolata po[tesse] evitare eccessive restrizioni ai fini dell'accertamento della verità, tenuto conto del continuo sviluppo tecnologico che estende le frontiere dell'investigazione, senza mettere in pericolo le garanzie difensive»[80].

Anche l'impiego del termine "assunzione" non avrebbe una rilevanza decisiva, in quanto, oltre a ricorrere nell'art. 188 c.p.p., che viene pacificamente ritenuto applicabile anche agli atti

[77] Per una riflessione sul tema, si veda S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 257 e ss, la quale, col fine di sostenere l'opinione contraria a tale posizione, ne riporta comunque le argomentazioni.

[78] Così, G. RICCIO, *Ragionando su intelligenza artificiale*, op. cit., p. 7.

[79] *Relazione al Progetto preliminare del codice di procedura penale*, in *Gazzetta Ufficiale*, suppl. ord. n. 93, 24 ottobre 1988, p. 60.

[80] *Idem*, p. 60. Inoltre, sul punto, il legislatore fa anche esplicito riferimento al mezzo di ricerca della prova delle «tavole d'ascolto idonee ad accertare conversazioni tra presenti» (p. 60).

investigativi, andrebbe letto nel senso di "ammissione". Il giudice, dunque, potrebbe pronunciarsi sull'ammissibilità di uno strumento d'indagine informatico che rispetti le stesse garanzie poste dalla norma in questione, in tal modo facendo diventare il confronto tra le parti un contraddittorio *per* la prova e non solo sulla prova[81]. La stessa giurisprudenza, proprio sul punto, arriva ad ammettere che l'art. 189 c.p.p. sia applicabile anche alle indagini atipiche perché «il contraddittorio previsto dall'art. 189 c.p.p. non riguarda la ricerca della prova, ma la sua assunzione e interviene, dunque, […] quando il giudice è chiamato a decidere sull'ammissione della prova»[82].

Da ultimo, la necessità di svolgere un contraddittorio potrebbe essere salvaguardata posticipando il momento in cui questo avviene. Infatti, imporre un confronto anticipato tra le parti, in sede di indagini preliminari, andrebbe a sicuro detrimento dell'efficacia stessa delle indagini. Proprio «attraverso una lettura fluida della norma»[83], si potrebbe propendere per uno svolgimento a posteriori[84] del contraddittorio tra le parti avendo ad oggetto la tutela della libertà morale e l'idoneità accertativa dell'indagine atipica.

Il criterio dell'idoneità accertativa verte sul metodo scientifico utilizzato, ma deve essere verificato tanto sul piano dell'astrattezza quanto su quello della concretezza. Come è stato osservato, in astratto, «verrebbero in rilievo la sua verificabilità e, quindi, la possibilità di effettuarne un controllo; la sua credibilità, che sarebbe avvalorata dall'esito negativo che abbiano sortito i tentativi di falsificazione; la percentuale di errore, nonché l'accreditamento che il metodo impiegato riceve presso la comunità scientifica di riferimento»[85]. Invece, in concreto si rende necessario verificare la genuinità delle fonti di prova raccolte[86], dato che, come visto, gli strumenti informatici e i dati da questi elaborati sono vulnerabili e oggetto di possibili tentativi di alterazione (soprattutto, da parte della criminalità).

In generale, lo scrivente ritiene che, nel momento in cui si utilizzano strumenti tecnici di investigazione, gli elementi di prova raccolti non siano sempre idonei ad assicurare l'accertamento

---

[81] Cfr. Cfr. G. CANZIO, *Intelligenza artificiale*, op. cit., par. 5. L'Autore ritiene che questo contraddittorio *per* la prova dovrebbe avere la funzione, quale filtro di accesso, di escludere che nel patrimonio probatorio entrino informazioni non sorrette da legittima validazione giuridica. Tuttavia, la paternità dei concetti di contraddittorio per la prova e sulla prova va al giurista D. SIRACUSANO, che ha proposto l'efficace distinzione nell'ambito del convegno *Dal processo inquisitorio al processo accusatorio. Luci ed ombre di una svolta epocale*, Torino 25 luglio 2013 (reperibile online al collegamento https://www.radioradicale.it/scheda/386423/dal-processo-inquisitorio-al-processo-accusatorio-luci-ed-ombre-di-una-svolta-epocale, consultato da ultimo in data 21 giugno 2022).

[82] Così, in tema di riprese visive, Cassazione penale, Sez. un., sentenza «Prisco» cit., p. 12.

[83] In tali termini, S. SIGNORATO, *Le indagini digitali*, op. cit., p. 258.

[84] Cfr. A. CAMON, *Le riprese visive come mezzo d'indagine*, op. cit., pp. 1195, per il quale il contraddittorio potrebbe vertere su «una valutazione ed eventualmente una critica del procedimento» seguito dagli investigatori.

[85] In questi termini, S. SIGNORATO, *La localizzazione satellitare*, op. cit., p. 592. Vengono quindi richiamati i criteri Daubert cit. per la valutazione di affidabilità di un metodo scientifico in sede di ammissione della prova scientifica.

[86] La necessità di un accertamento sull'idoneità in concreto si può trarre dalla stessa *Relazione al Progetto preliminare del codice di procedura penale*, cit., p. 60, ove si afferma, in relazione all'art. 189 c.p.p., che il giudice deve verificare che le prove atipiche siano «affidabili sul piano della genuinità dell'accertamento e non lesive della libertà morale della persona».

dei fatti, ma concorda con chi sostiene che gli stessi non pregiudichino la libertà morale – dunque, non condizionino i comportamenti – delle persone coinvolte nelle indagini[87]. Tuttavia, vi possono essere dei casi in cui si realizzerebbe un pregiudizio per la libertà morale delle persone oggetto del controllo: come è stato osservato, il riconoscimento facciale effettuato in funzione di polizia predittiva attraverso un'elaborazione dati di cui non sono disciplinati né i criteri, né i fini metterebbe «a rischio la stessa libertà morale della persona fonte di prova, intesa come facoltà di autodeterminarsi rispetto agli stimoli»[88].

È vero che la mancanza di una normativa *ad hoc* sulla funzione dinamica di riconoscimento facciale impedisce, allo stato, di utilizzare legittimamente tale funzione di polizia predittiva per fini investigativi o processuali[89]; tale lacuna, però, determinerebbe una lesione al diritto di *privacy*, ma non arrecherebbe pregiudizio alla libertà morale, che, per lo scrivente, deve intendersi in senso più rigoroso[90]. Il rischio per il diritto alla *privacy* si anniderebbe nella possibile attuazione di una sorveglianza generalizzata, dovuta proprio dalla mancata indicazione dei criteri per eseguire il riconoscimento facciale in tempo reale. Tale controllo indiscriminato e sganciato da ogni previsione normativa si tradurrebbe in un'attività contraria al principio di proporzionalità, dunque illegittima.

L'attività di regolazione richiesta per questa attività specifica, tuttavia, è necessaria per trovare un bilanciamento tra le esigenze della sicurezza e il diritto alla *privacy* e rispettare così il principio di proporzionalità presente nel nostro sistema penale; ad ogni modo, la presenza di una disciplina *ad hoc* sulle modalità della messa in pratica dell'atto investigativo non è sempre necessaria, soprattutto quando si tratti di impiegare degli strumenti investigativi atipici caratterizzati da una basso grado di intrusività. Infatti, rispettati i due criteri di cui all'art. 189 c.p.p. e previsto un contraddittorio – per quanto posticipato – sulle modalità acquisitive dei materiali probatori ottenuti per mezzo di strumenti non tipici di ricerca della prova, le indagini svolte attraverso questi strumenti digitali possono essere qualificabili quali atti di indagini atipici e, di conseguenza,

---

[87] Cfr., W. NOCERINO, *Il tramonto dei mezzi di ricerca della prova nell'era 2.0*, in *Diritto penale e processo*, n. 8/2021, p. 1025. L'Autrice, tuttavia, ritiene che gli elementi di prova raccolti mezzo di strumenti investigativi digitali siano sempre idonei ad assicurare l'accertamento dei fatti.

[88] In questi termini, M. TORRE, *Nuove tecnologie e trattamento dei dati personali*, op. cit., pp. 1054, trattando della modalità di acquisizione dinamica del SARI Real Time.

[89] Cfr. Garante Privacy, parere n. 127/2021 cit.

[90] Il Gruppo Indipendente nominato dalla Commissione europea nel 2019 ha affermato che, nei confronti dell'intelligenza artificiale, «il rispetto per la dignità umana implica che tutte le persone siano trattate con il rispetto loro dovuto in quanto *soggetti* morali, piuttosto che come semplici *oggetti* da vagliare, catalogare, valutare per punteggio, aggregare, condizionare o manipolare» (*Orientamenti etici per un'IA affidabile*, op. cit., Punto 41, p. 12). Si veda Capitolo I, nota n. 79. Lo scrivente è ben conscio che l'attività compiuta dal SARI in modalità dinamica faccia sembrare l'uomo come un oggetto da vagliare e catalogare, ma ritiene che si possano superare queste criticità con la predisposizione di una normativa che la disciplini, vista l'importanza ricoperta dal settore della prevenzione e repressione del crimine. Per questo motivo, considera violata la dignità umana solo di fronte a un'attività che, nel concreto ed effettivamente, incida e vincoli l'autodeterminazione altrui.

ammissibili anche se non disciplinati esplicitamente dalla legge[91] (anche di natura regolamentare).

A questo punto, verificati il rispetto a monte, del diritto alla *privacy* e del principio dell'equità del processo nel suo complesso, per come intesi dalla Corte EDU (come detto, l'art. 2 Cost. non prevede alcun tipo di garanzia nel riconoscere diritti emergenti), e la rispondenza dell'attività d'indagine ai criteri stabiliti dall'art. 189 c.p.p., si può ritenere che l'atto d'indagine atipico svolto detenga i requisiti minimi richiesti dall'ordinamento per essere considerato ammissibile e, quindi, che gli elementi di prova acquisiti attraverso di esso possano essere presi in considerazione dal giudice nella fase decisoria.

Dunque, la valutazione probatoria non può mai prescindere dalle regole contenute all'interno del codice di rito sull'utilizzabilità agli artt. 191 e 526 c.p.p.[92], giungendo altrimenti alla conclusione illogica di porre alla base di una decisione elementi di prova inutilizzabili.

Allo stesso modo di tutte le altre prove, la rilevanza probatoria dei risultati degli algoritmi dovrà essere delimitata e non considerata intrinsecamente privilegiata. Questi, oltre ad essere rimessi alla libera valutazione del giudice (che non può appiattirsi su quanto deciso dalla macchina) ai sensi dell'art. 192, co. 1 c.p.p., dovranno anche rispondere alle regole previste dal co. 2 in merito agli indizi: di conseguenza, i risultati dell'elaborazione informatica potranno rilevare a patto che siano «gravi, precisi e concordanti» ovvero consentano di ricostruire il fatto oggetto delle indagini in senso univoco e, comunque, tale da escludere altre ragionevoli ipotesi[93].

---

[91] Cfr. W. NOCERINO, *Il tramonto dei mezzi di ricerca della prova*, cit., p. 1025. Tuttavia, la stessa Autrice (*infra*, p. 1030) ritiene che, per evitare l'ammissibilità di indagini atipiche ai limiti della costituzionalità, si «si potrebbe propendere per l'introduzione di un nuovo mezzo di ricerca della prova ("intrusione informatica", potrebbe definirsi) per regolare le attività di accesso, osservazione e acquisizione di dati e informazioni da remoto, esperibile mediante l'impiego di sempre più sofisticate tecniche di indagine. In questi casi, non sarebbe tipizzato lo strumento con cui condurre le indagini informatiche quanto piuttosto le regole cui ricorrere ogni qual volta si proceda ad attività di sorveglianza occulta e continuativa da remoto, predisponendo le garanzie fondamentali che devono essere sempre riconosciute all'indagato e ai soggetti terzi occasionalmente coinvolti, a prescindere dalla tecnica investigativa impiegata. In altre parole, l'obiettivo potrebbe essere quello di introdurre una nuova categoria probatoria, con la quale verrebbero individuati i "casi" e i "modi" dell'ingerenza nella sfera privata degli individui, in modo da ritenere il sacrificio dei diritti inviolabile assolutamente rispettoso al principio di stretta legalità e al principio di proporzione. Con ciò non si intende "imbrigliare" in un eccessivo formalismo giuridico le attività di polizia ma solo rendere conforme ai principi propri di uno Stato di diritto un sistema che, ad oggi, è ancora orfano di regole».

[92] Cfr. D. POLIDORO, *Tecnologie informatiche e procedimento penale*, op. cit., p. 11. Analogamente, C. PARODI – V. SELLAROLI, *Sistema penale e intelligenza artificiale*, op. cit., p. 58.

[93] Cfr. D. POLIDORO, *ult. cit.*, p. 11.

CONCLUSIONI

Al termine dell'analisi svolta, si può giungere alla conclusione per cui l'uso di dispositivi di intelligenza artificiale con finalità di prevenzione del reato va incoraggiato, ferme restando le necessità di garantire determinate tutele, ribadire la centralità dell'uomo e limitare l'uso di tali strumenti ad un ruolo ancillare.

Anche se calibrate per campi diversi, le varie Carte etiche per un'IA a misura d'uomo che sono state esaminate concordano nel porre l'attenzione su alcune tematiche comuni, quali il rispetto dei diritti fondamentali e dell'autonomia umana, la trasparenza e l'esplicabilità dei dispositivi informatici e l'opportunità che gli strumenti informatici non possano determinare la diretta produzione di effetti nella sfera giuridica dell'interessato, dovendosi riservare tale potere solo all'uomo.

Come visto, l'indicazione di questi e altri principi per l'utilizzo di dispositivi di IA non si traduce in un mero esercizio di catalogazione astratta; in realtà, la loro concreta attuazione evita che le attività messe in essere attraverso gli stessi non siano rispettose del divieto di non discriminazione, del diritto alla *privacy* e del principio del giusto processo, che si esplica principalmente nei suoi corollari del diritto di difesa e della parità delle armi.

La necessità, tanto in ambito amministrativo quanto in quello penale, di affrontare in modo risolutivo il problema dell'opacità algoritmica col fine di garantire trasparenza ed esplicabilità dei dispositivi diventa, quindi, cruciale: l'eventuale diffusione di strumenti informatici di cui sia ignoto il funzionamento (cd. scatole nere) sarebbe inaccettabile perché, di fatto, intaccherebbe tutti quei principi che fanno da architrave all'ordinamento giuridico che conosciamo.

Più che altro, tenuti fermi i principi che guidano i vari campi giuridici in cui di volta in volta gli algoritmi vengono utilizzati, la qualità e la scelta dei dati, la trasparenza del metodo di elaborazione degli stessi e gli scopi a cui indirizzare questi strumenti tecnologici sono la chiave per garantire una loro introduzione ponderata nel sistema giuridico. Come è stato osservato anche in merito agli algoritmi di polizia predittiva, «*[c]riminal law can do little*, *in this perspective*: […] *scientific validity, accessibility and transparency are the parameters for measuring the riability of these instruments, not the principles of criminal law*»[1].

L'essere umano, infatti, deve rimanere il modello in funzione del quale vengono costruiti gli algoritmi di IA e il soggetto beneficiario delle loro elaborazioni. Non si ritiene, quindi, opportuno

[1] Tradotto: «[l]a legge penale può fare poco, in questa prospettiva: validazione scientifica, accessibilità e trasparenza sono i parametri per la misurazione dell'affidabilità di questi strumenti, non i principi della legge penale». Così, S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., p. 40.

che per i dispositivi informatici siano previsti margini di autonomia tali da determinare effetti giuridici diretti nella sfera degli interessati, se non nella misura in cui si tratti di attività vincolate da chiari parametri a monte e sia sempre il responsabile umano del procedimento a far propria la decisione algoritmica, a seguito di un controllo significativo e di un'effettiva rielaborazione della stessa. Questo non significa, soprattutto per quanto riguarda gli strumenti d'indagine, che l'uomo non possa essere oggetto, inteso come destinatario, della loro attività, ma che ciò debba avvenire solo nel momento in cui a tale oggetto siano riconosciuti – *rectius*, ribaditi in "versione digitale" – e resi concretamente esercitabili i diritti tradizionalmente previsti, oltre ai nuovi diritti.

Per giungere a tali obiettivi, determinante diviene l'intervento di ricercatori e studiosi nella produzione di studi pertinenti destinati a chi prende decisioni pubbliche per certificare, già dalla prima fase d'implementazione e messa a punto, la rispondenza del funzionamento di tali algoritmi a principi etici e giuridici. Tra l'altro, questo controllo deve proseguire anche dopo l'inizio dell'attività dello strumento, facendo in modo che, con il costante aggiornamento e l'adozione di correttivi, lo stesso non finisca per operare *contra legem* indisturbatamente a causa della presunta aurea di infallibilità che connota i dispositivi informatici.

Anche se l'art. 11 Direttiva (UE) n. 2016/680 ammette la possibilità che una decisione basata unicamente su un trattamento automatizzato possa produrre effetti giuridici negativi sull'interessato, quando questa sia autorizzata dal diritto dell'Unione europea o dello stato membro e siano previste garanzie adeguate, l'interpretazione sistematica preferibile è quella che ritiene necessario un intervento umano qualificato e significativo nel valutare le risultanze algoritmiche e darne eventualmente attuazione. I dispositivi di IA, dunque, non possono essere utilizzati se non in funzione di ausilio per l'uomo.

Per quanto riguarda gli strumenti di polizia predittiva, dapprima si è dimostrato come le critiche avanzate sul loro funzionamento non possano tradursi in un loro rifiuto totale, ma debbano rivolgersi contro specifiche modalità operative (il riferimento è ai dispositivi *hotspot*) ed eventuali vizi inerenti ai dati utilizzati; in seconda battuta, sono state fatte diverse considerazioni, in base al fatto che i risultati prodotti dall'elaborazione algoritmica possano o meno essere impiegati anche nell'ambito delle attività di polizia giudiziaria e, dunque, essere validamente posti a fondamento di una decisione giurisdizionale.

Da un lato, le attività di polizia di prevenzione per mezzo di algoritmi predittivi possono essere ritenute efficaci fin tanto che riescono ad anticipare la commissione di un delitto o favoriscono l'arresto in flagranza dell'autore. Ribadita la necessità di utilizzare dati provenienti da fonti affidabili e sicure per avere un'elaborazione informatica di qualità, «non sembra sussistere, in tali casi, alcuna problematica sostanziale – quantomeno sul piano processuale […] – poiché, tanto il

principio di materialità, quanto il principio di offensività sembrano rappresentare idonei ed adeguati argini rispetto alla circostanza che l'impiego degli algoritmi in discorso possa alimentare una deriva del giudizio penale verso la punibilità delle mere volontà criminali, piuttosto che delle condotte concretamente poste in essere da un determinato individuo»[2]. Dall'altro lato, invece, quando i risultati dell'elaborazione algoritmica possono avere una rilevanza nelle attività della polizia giudiziaria, si impongono esigenze di tutela dell'accertamento probatorio.

Circa i temi dell'ammissibilità ed utilizzabilità nel processo degli esiti dei calcoli matematici di un programma informatico per ricondurre la responsabilità penale in capo ad un soggetto, si è visto come la disciplina offerta dall'art. 189 c.p.p. sulle prove atipiche possa venire in soccorso nel tentativo di non disperdere informazioni utili per l'esito del processo raccolte e/o elaborate per il tramite di mezzi di ricerca della prova atipici, quali sono i nuovi strumenti tecnologici. I requisiti lì richiesti, però, devono essere interpretati con una certa flessibilità (ad esempio, ammettendo, forse forzando il dettato normativo, che il confronto tra le parti sulla prova possa essere postumo) e integrati con le tutele indicate dagli artt. 6 e 8 CEDU, non potendosi riscontrare alcuna indicazione o limitazione nell'ambito dell'art. 2 Cost., all'interno del quale, ormai, viene ricondotta tutta una serie di diritti emergenti (ad esempio, il diritto all'esplicabilità dell'algoritmo) legati all'utilizzo di dispositivi di IA. Solo a questo punto, potranno essere oggetto di valutazione nel merito del giudice ai sensi dell'art. 192 del codice di rito.

Tuttavia, per evitare che il tema della validità della raccolta e dell'elaborazione di prove per mezzo di algoritmi sia lasciato esclusivamente all'interpretazione estensiva degli operatori del diritto, è auspicabile un intervento del legislatore volto a disciplinare i presupposti e le modalità operative di questa particolare specie di indagini digitali. In questo modo, sarebbero stabiliti a monte un equilibrio tra i diritti lesi e l'interesse al perseguimento della giustizia, dei criteri di proporzionalità tra lesione-limitazione, delle regole sull'ulteriore elaborazione dati eventualmente richiesta dagli strumenti per funzionare (come nel caso del SARI in modalità dinamica) e l'eventuale previsione di una preventiva autorizzazione giurisdizionale delle attività d'indagine, evitando così che queste si traducano in atti contrari ai principi costituzionali.

Invece, nel tentativo di reprimere gli specifici reati legati alla corruzione, l'uso di strumenti di polizia predittiva non si rileva adatto: infatti, questi dispositivi, dovendo attingere a una gran mole di dati per continuare a elaborare delle previsioni, si rilevano efficaci solo nei confronti dei crimini seriali. Con i fenomeni corruttivi, invece, si pone il problema non risolvibile di recuperare una significativa quantità di informazioni con cui far funzionare un *software* così impostato, in quanto l'interesse di tutte le parti partecipanti al *pactum sceleris* è che il fatto rimanga occulto.

[2] In questi termini, D. POLIDORO, *Tecnologie informatiche e procedimento penale*, op. cit., p. 10.

Tuttavia, per svolgere questo compito, sono stati realizzati dei particolari algoritmi (*Big data analytics*), che segnalano degli indicatori di anomalia e rischio su uno specifico procedimento amministrativo rispetto ad un modello e a criteri di raffronto medi; oppure, che monitorano il traffico di posta elettronica riferibile a un dipendente, allo scopo di individuare conversazioni ipoteticamente riferibili a fenomeni corruttivi o di mala amministrazione in atto. Ad ogni modo, allo stato non è nota alcuna sperimentazione in atto di tali strumenti all'interno della pubblica amministrazione italiana, anche se l'Autorità Nazionale Anticorruzione ha già posto le basi perché sia intrapresa questa via, elaborando opportuni indicatori statistici di sintesi (*red flags*) capaci di indirizzare l'attività di vigilanza in modo mirato verso situazioni potenzialmente di maggiore criticità.

Nell'ottica di diffusione di tali algoritmi, questi, se ordinariamente previsti, dovranno rispettare gli adempimenti imposti dall'art. 4 dello Statuto dei lavoratori, salvo che, di fronte a concreti indizi, non rientrino in un'operazione di sorveglianza occulta volta a raccogliere prove dell'infedeltà del dipendente. L'impiego di tali algoritmi potrebbe essere previsto, per le aziende private, all'interno dei modelli 231 e, per le pubbliche amministrazioni, nel nuovo Piano Integrato di Attività e Organizzazione di cui all'art. 6 D.L. 80/2021.

Per lo specifico ambito pubblico, tuttavia, la completa realizzazione della Piattaforma Nazionale Digitale Dati di cui all'art. 50-*ter* CAD diventa attività basilare per risolvere il problema della mancata interoperabilità tra le diverse banche dati pubbliche e permettere ai *big data analytics* di incrociare dati eterogenei da cui trarre informazioni per finalità di anticorruzione.

Ad ogni modo, anche la trasparenza è, in senso lato, diventata strumento per combattere la corruzione e favorire un controllo esterno sul buon andamento della cosa pubblica. Se la corruzione penalmente rilevante si combatte con la repressione e l'uso di strumenti tecnologici, quale il captatore informatico (*trojan*), le forme di malcostume riguardanti il diritto amministrativo si affrontano con meccanismi organizzativi e procedurali, agendo sui controlli amministrativi e sulla trasparenza, puntando sulla deontologia e sulla formazione del personale. In generale, anche l'uso dell'intelligenza artificiale può, dunque, rientrare tra quei meccanismi organizzativi volti a scoraggiare la nascita di fenomeni corruttivi.

Al di là della predisposizione di strumenti e misure preventivi e repressivi per combattere il crimine, ciò che resta difficile da capire sono i motivi per cui nascono questi fenomeni. In merito ai reati contro la PA, questi sicuramente si annidano nella mancanza di senso delle istituzioni, di senso del dovere personale, di motivazione rispetto al lavoro che si svolge e nella mancata percezione del benessere collettivo come valore in sé. L'unico modo per arginare simili comportamenti è, dunque,

quello di puntare sull'istruzione e la cultura[3]: «*officii fructus sit ipsum officium*»[4].

[3] Specificamente per l'ambito anticorruzione, Cfr. OSCE, *Prevenzione e lotta alla corruzione attraverso la digitalizzazione*, op. cit., Punto 1.i.

[4] Tradotto: «il premio del dovere sia il dovere medesimo». Così, M.T. CICERONE, *Retorica*, *De finibus*, Libro II, par. 72.

BIBLIOGRAFIA

AA.VV., *State v. Loomis. Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing*, in *Harvard Law Review*, Vol. 130, 2017.

AGCM – AGCOM – GARANTE PRIVACY, *Indagine conoscitiva sui* Big Data, 2020.

AARVIKPP P. (a cura di), *Artificial Intelligence – a promising anti-corruption tool in development settings?*, in www.u4.no, Report n. 1/2019, U4 Brief, n. 7/2018, U4 Anti-Corruption Resource Centre, Bergen 2019.

AGID – TASK FORCE IA, *Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino*, 2018.

AGID, *Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati*, ai sensi dell'articolo 50-ter, comma 2 del CAD, 2021.

AI4People, *An Ethical Framework for a Good IA Society: Opportunities, Risks, Principles, and Recommendations*, 2018.

AKPINAR N. – DE-ARTEAGA M. – CHOULDECHOVA A., *The effect of differential victim crime reporting on predictive policing systems*, in *FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, Association for Computing Machinery, New York 2021, pp. 838-849.

ALGERI L., *Intelligenza artificiale e polizia predittiva*, in *Diritto penale e processo*, n. 6/2021, pp. 724-734.

ANAC, MARINO G. – SBICCA F. (a cura di), *Efficienza dei contratti pubblici e sviluppo di indicatori di rischio corruttivo*, 2018.

ANAC, *Piano nazionale anticorruzione 2019.*

ANAC, *La corruzione in Italia (2016-2019). Numeri, luoghi e contropartite del malaffare*, 2019.

ANAC, *Esame e commento degli articoli del decreto-legge 16 luglio 2020, n. 76 «Misure urgenti per la semplificazione e l'innovazione digitale» in tema di contratti pubblici, trasparenza e anticorruzione*, 4 agosto 2020.

ANGWIN J. – LARSON J. – MATTU S. – KIRCHNER L., *Machine Bias*, in www.propublica.org, 23 maggio 2016.

ASIMOV I., *Girotondo*, in I. ASIMOV, *Io, Robot*, Bompiani, 1963, pp. 43-72.

ANGELINI R., *Intelligenza Artificiale e* governance*. Alcune riflessioni di sistema*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione,* Giappichelli Editore, Torino 2018, pp. 293-318.

BABUTA A. – OSWALD M., *Data Analytics and Algorithms in Policing in England and Wales*, Royal United Services Institute, London 2020.

BACCARI G.M. – CONTI C., *La corsa tecnologica tra Costituzione, codice di rito e norme sulla* privacy*: uno sguardo d'insieme*, in *Diritto penale e processo*, n. 6/2021, PP. 711-723.

BARBARO C., *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?*, in www.questionegiustizia.it, n. 4/2018, pp. 189-195.

BARBARO C. (a cura di), *Cepej, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (IA) nei sistemi giudiziari*, in www.questionegiustizia.it, 7 dicembre 2018.

BARBARO C., *Lo studio di fattibilità di un nuovo quadro normativo sulla concezione, lo sviluppo e l'applicazione dei sistemi di Intelligenza Artificiale sulla base delle norme del Consiglio d'Europa. Il lavoro del Comitato Ad hoc sull'intelligenza artificiale del Consiglio d'Europa (CAHAI)*, in www.questionegiustizia.it, 28 aprile 2021.

BARENDRECHT M., *Rechtwijzer: Why Online Supported Dispute Resolution Is Hard to Implement*, in www.hiil.org, 21 giugno 2017.

BASILE F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto Penale e Uomo* (DPU), 2019, n. 10.

BASSINI M. – LIGUORI L. – POLLICINO O., *Sistemi di Intelligenza Artificiale, responsabilità e* accountability*. Verso nuovi paradigmi?*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione,* Giappichelli Editore, Torino 2018, pp. 333 e ss.

BENEDETTI D., *IA e (in)sicurezza informatica*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione,* Giappichelli Editore, Torino 2018, pp. 239-264.

BENETAZZO C., *ANAC e sistema europeo dei contratti pubblici*, Giappichelli Editore, Torino 2020.

BENETAZZO C., *Intelligenza artificiale e nuove forme di interazione tra cittadino e pubblica amministrazione*, in www.federalismi.it, n. 16/2020, pp. 24-35.

BENETAZZO C., *Gli appalti pubblici nel PNRR tra semplificazione e prevenzione della corruzione*, in www.federalismi.it, n. 29/2021, pp. 122-134.

BENNETT MOSES L. – CHAN J., *Algorithmic prediction in policing: assumptions, evaluation, and accountability*, in *Policing and Society*, vol. 28, n. 7/2018.

BERLINER D. – DUPUY K., *The promise and perils of data for anti-corruption efforts in international development work*, in www.u4.no, U4 Brief, n. 7/2018, U4 Anti-Corruption Resource Centre, Bergen 2018.

BIERMANN K., *Noch hat niemand bewiesen, dass Data Mining der Polizei hilft*, in www.zeit.de, 29 marzo 2015.

BIRRITTERI E., Big Data Analytics *e* compliance *anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2019, pp. 289-303.

BIRRITTERI E., *Controllo a distanza del lavoratore e rischio penale*, in *Sistema penale*, 2021.

BOLOGNINI L., *Codice etico UE sull'intelligenza artificiale: forte la tecnica, debole la politica*, in www.focus.it, 2 gennaio 2019.

BONFANTI A., Big data *e polizia predittiva: riflessioni in tema di protezione del diritto alla* privacy *e dei dati personali*, in www.medialaws.eu (*Rivista di diritto dei media*), n. 3/2018.

BONINI V., *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in *Processo penale e giustizia*, n. 2/2019, pp. 338-348

BONTEMPELLI M., *Il captatore informatico in attesa della riforma*, in *Diritto Penale Contemporaneo*, 20 dicembre 2018.

BORGOBELLO M., *Il procuratore "robot" debutta in Cina: così l'IA ora elabora le accuse*, in www.agendadigitale.eu, 14 gennaio 2022.

CAHAI, *Feasibility Study*, 17 dicembre 2020.

CALABRÒ V. – COSTABILE G. – FRATEPIETRO S. – IANULARDO M. – NICOSIA G., *L'alibi informatico. Aspetti tecnici e giuridici*, in *IISFA Memberbook*, Experta, Forlì 2010, pp. 297-328.

CALAVITA O., *L'odissea del* Trojan Horse, in *Diritto Penale Contemporaneo*, fasc. n. 11/2018.

CAMALDO L., *Le innovazioni previste dalla legge anticorruzione in tema di intercettazioni con captatore informatico*, in *Diritto Penale Contemporaneo*, 24 settembre 2019.

CAMON A., *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cassazione penale*, 1999, pp. 1192-1213.

CAMON A., *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Rivista italiana di diritto e procedura penale*, n. 2/2005, pp. 594-650.

CAMON A., *Le Sezioni Unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni nuovi dubbi*, in *Rivista italiana di diritto e procedura penale*, 2006, pp. 1550-1569.

CAMON A., *Captazione di immagini (diritto processuale penale)*, in *Enciclopedia del diritto. Annali, vol. VI*, Giuffré, Milano 2013, pp. 133-149.

CANESCHI G., *Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2019, pp. 417-429.

CANZIO G., *Intelligenza artificiale, algoritmi e giustizia penale*, in www.sistemapenale.it, 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 of Case Configurations to Explore the Dynamics of Criminogenic Behavior Settings*, in *Journal of Contemporary Criminal Justice*, vol. 33, n. 2/2017, pp. 133-151.

CAPORALE M., *Dalle* smart cities *alla cittadinanza digitale*, in www.federalismi.it, n. 2/2020, pp. 29-46.

CARIOLA G., *Così la blockchain aggiorna i controlli interni*, in www.ntplusfisco.ilsole24ore.com (*Quotidiano del Fisco* – il Sole24ore), 16 febbraio 2019.

CARRER S., *Se l'*amicus curiae *è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin*, in www.giurisprudenzapenale.com, n. 4/2019.

CASTELLI C., *Giustizia predittiva*, in www.questionegiustizia.it, 8 febbraio 2022.

CASTELLI C. – PIANA D., *Giustizia predittiva. La qualità della giustizia in due tempi*, in www.questionegiustizia.it, 15 maggio 2018.

CASTELLI C. – PIANA D., *Giusto processo e intelligenza artificiale*, Maggioli Editore, Rimini 2019.

CASTETS-RENARD C. – BESSE P. – LOUBES J. – PERRUSSEL L., *Encadrement des risques techniques et juridiques des activités de police prédictive*, [Rapport de recherche] Centre des Hautes Etudes du Ministère de l'Intérieur, 2019.

CATH C. –WACHTER S. –MITTELSTADT B. –TADDEO M. – FLORIDI L., *Artificial Intelligence and the "Good Society": the US, EU, and UK approach*, in *Science and Engineering Ethics*, 2018.

CEPEJ, Studio n. 24, *Rapport thématique: l'utilisation des technologies de l'information par les tribunaux en Europe*, 2016.

CEPEJ, *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, 2019.

CERESA GASTALDO F., *Il giudice-robot: l'intelligenza artificiale nei sistemi giudiziari tra aspettative ed equivoci*, in www.iusinitinere.it, 22 marzo 2021.

CERESA GASTALDO F., *Lo statuto della giustizia digitale nella Carta etica della CEPEJ*, in www.iusinitinere.it, 2 aprile 2021.

CHEN S., *Is China's corruption-busting AI system "Zero Trust" being turned off for being too efficient?*, in *South China Morning Post*, 4 febbraio 2019.

CHEN S., *Chinese scientists develop AI 'prosecutor' that can press its own charges*, in *South China Morning Post*, 26 dicembre 2021.

CHRISTIE A., *La serie infernale*, Mondadori, Milano 2012, ed3. n. 35.

CICERONE M.T., *Retorica*, *De finibus*, Libro II, par. 72.

CLARIZIA P., *La digitalizzazione della pubblica amministrazione*, in *Giornale di diritto amministrativo*, n. 6/2020, pp. 768-781.

CNIL, *Comment permettre à l'homme de garder la main?*, 2017.

CONSIGLIO D'EUROPA – COMMITTEE OF EXPERTS ON INTERNET INTERMEDIARIES, *Algorithms and Human Rights. Study on the Human Rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*, 2017.

CONSIGLIO D'EUROPA – COMMISSARIATO PER I DIRITTI UMANI, *Unboxing Artificial Intelligence: 10 steps to protect Human Rights*, 2019.

COORTEL M., *Prospecter et punir: étude critique des logiciels Blue Crush et PredPol*, in *Encyclo. Revue de l'ecole doctorale ED 382*, Université Sorbonne Paris Cité, n. 7/2015.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo. Diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza*, aggiornata al 31 agosto 2019.

COSTANZI C., *La matematica del processo: oltre le colonne d'Ercole della giustizia penale*, in www.questionegiustizia.it, n. 4/2018, pp. 166-188.

CRUPI G., *XLAW – Innovazione strategica e tecnologica per la prevenzione dei reati predatori urbani*, in *Polizia – Periodico S.I.A.P.*, n. 69/2018.

CUOMO L. – GIORDANO L., *Informatica e processo penale*, in *Processo Penale e Giustizia*, fasc. n. 4/2017, pp. 716-731.

D'AGOSTINO L., *Sicurezza informatica, compliance e prevenzione del rischio di reato*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2019, pp. 354-373.

DALFINO D., *Stupidità (non solo) artificiale, predittività e processo*, in www.questionegiustizia.it, 3 luglio 2019.

DANIELE M., *La prova digitale nel processo penale*, in *Rivista di Diritto Processuale*, 2011, pp. 286 e ss.

DELLA TORRE J., *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice, in *Diritto Penale Contemporaneo*, n. 1/2020, pp. 231-247.

DELLA TORRE J., *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Rivista di diritto processuale*, n. 2/2021.

DE PETRIS G., *La digitalizzazione del Fisco e la difficile parità delle armi fra Amministrazione e contribuente*, in *Corriere Tributario*, n. 6/2020.

DICK P.K., *Rapporto di minoranza*, in *Rapporto di minoranza e altri racconti*, Fanucci, Roma 2002.

DI COSTANZO V., *Report K-crime: prevedere il crimine dal Key-Crime a Palantir*, in www.salvisjuribus.it, 27 settembre 2020.

DI GENNARO G. – LOMBARDO E. – MARSELLI R. – SPINA M., *Tolleranza zero o deterrenza selettiva: quali strade intraprendere per rispondere più efficacemente alla domanda di sicurezza*, in G. DI GENNARO – R. MARSELLI (a cura di), *Secondo Rapporto – Criminalità e Sicurezza a Napoli*, Federico II University Press, Napoli 2017.

DIETERICH W. – MENDOZA C. – BRENNAN T., *COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity*, 8 luglio 2016.

DONATI F., *Intelligenza artificiale e giustizia*, in C. BERTOLINO – T. CERRUTI – M. OROFINO – A. POGGI, *Scritti in onore di Franco Pizzetti*, Vol. II, Edizioni Scientifiche Italiane, 2020.

DORIGO S. (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini, Pisa 2020.

DREYFUS H. L., *What computers still can't do. A critique of artificial reason*, Harper & Row, New York 1972.

DRESSEL J. – FARID H., *The accuracy, fairness, and limits of predicting recidivism*, in *Science Advances*, vol. 4, n. 1/2018.

ENGSTROM D.F. – HO D.E. –SHARKEY C.M. –CUÉLLAR M.F. (a cura di), *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies. Report submitted to the Administrative Conference of the United States*, 2020.

ERRANTE V., *Cina, arrivano i robot-magistrati. Ora ti accusa un algoritmo: «Decide col 97% di precisione»*, in www.ilmessaggero.it, 2 gennaio 2022.

FALCONE M., *La* big data analytics *per conoscere, misurare e prevenire la corruzione*, in M. GNALDI – B. PONTI (a cura di), *Misurare la corruzione oggi*, Franco Angeli, Milano 2018, pp. 90-110.

FASANO G., *L'intelligenza artificiale nella cura dell'interesse generale*, in *Giornale di Diritto Amministrativo*, n. 6/2020, pp. 715-726.

FAZEKAS M. – DÁVID-BARRETT E., *Corruption Risks in UK Public Procurement and New Anti-Corruption Tools,* Government Transparency Institute, Budapest 2015.

FLORES 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*, vol. 80, n. 2/2016, pp. 38-46.

FLORIDI L., *What the Near Future of Artificial Intelligence Could Be*, in *Philosophy & Technology*, 2019, n. 32.

FLORIDI L. – COWLS J. – BELTRAMETTI M. – CHATILA R. – CHAZERAND P. – DIGNUM V. – LUETGE C. – MADELIN R.– PAGALLO U. – ROSSI F. – SCHAFER B. – VALCKE P. – VAYENA E.J.M., "*AI4People – An Ethical Framework for a Good IA Society: Opportunities, Risks, Principles, and Recommendations*", in *Minds and Machines*, vol. 28, n. 4/2018.

FONDAZIONE LEONARDO – CIVILTÀ DELLE MACCHINE, *Statuto Etico e Giuridico dell'IA*, 2019.

FONSI A., *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in www.penaledp.it, 14 maggio 2021.

FUTURE OF LIFE INSTITUTE, *Asilomar AI Principles*, 2017.

GABORIAU S., *Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?*, in www.questionegiustizia.it, n. 4/2018, pp. 200-212.

GALATI A., *L'avvento della tecnologia nelle aule giudiziarie: può il destino della giustizia essere affidato ad un algoritmo?*, in www.iusinitinere.it, 6 agosto 2020.

GALETTA D.U., *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in *Rivista Italiana di Diritto Pubblico Comunitario*, fasc. n. 3/2020, pp. 501 e ss.

GALETTA D.U. – CORVALÁN J.G., *Intelligenza Artificiale per una pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in www.federalismi.it, n. 3/2019.

GAUTHIER F., *Prédire les vols de voitures?*, in www.etalab.gouv.fr, 12 gennaio 2018.

GAZZOLO T., Minority Report *e il crimine senza crimine*, in www.jus.vitaepensiero.it, vol. 6, n. 1/2020.

GIALUZ M., *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto Penale Contemporaneo*, 29 maggio 2019.

GIORDANO L., *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *Sistema penale*, n. 4/2020, pp. 109-143

GNALDI M., *Indicatori di corruzione e nuovi indicatori di prevenzione della corruzione*, in M. GNALDI – B. PONTI (a cura di), *Misurare la corruzione oggi*, Franco Angeli, Milano 2018, pp. 31-46.

GRIFFO M., *Il* trojan *e le derive del terzo binario*, in *Sistema penale*, n. 2/2020, pp. 61-70.

GRUPPO EUROPEO PER L'ETICA DELLE SCIENZE E DELLE NUOVE TECNOLOGIE, *Statement on artificial intelligence, robotics and "autonomous" systems*, 9 marzo 2018.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 ed emendata il 6 febbraio 2018.

GRUPPO INDIPENDENTE DI ESPERTI AD ALTO LIVELLO SULL'INTELLIGENZA ARTIFICIALE ISTITUITO DALLA COMMISSIONE EUROPEA NEL GIUGNO 2018, *Una definizione di IA: principali capacità e discipline scientifiche*, aprile 2019.

GRUPPO INDIPENDENTE DI ESPERTI AD ALTO LIVELLO SULL'INTELLIGENZA ARTIFICIALE ISTITUITO DALLA COMMISSIONE EUROPEA NEL GIUGNO 2018, *Orientamenti etici per un'IA affidabile*, 8 aprile 2019.

GUARRIELLO V., *I sistemi di intelligenza artificiale in uso alle Forze dell'Ordine in Italia*, in www.salvisjuribus.it, 10 maggio 2020.

GULLO A., *Note minime sul rapporto tra diritto amministrativo e diritto penale*, in *Luiss Law Review*, n. 2/2018, p. 39.

HALLEVY G., *Liability for Crimes Involving Artificial Intelligence Systems*, Switzerland 2014.

HAMMOND K., *5 unexpected sources of bias in artificial intelligence*, in www.techcrunch.com, 10 dicembre 2016.

HEAVEN W.D., *Predictive policing is still racist – whatever data it uses*, in www.technologyreview.com, 5 febbraio 2021.

HOUSE OF COMMON – COMITATO SULLA SCIENZA E TECNOLOGIA, *Algorithms in decision-making. Fourth Report of Session 2017-2019*, 23 maggio 2018.

HOUSE OF LORDS – COMITATO SULL'INTELLIGENZA ARTIFICIALE, *AI in the UK: ready, willing and able?*, 2018.

HUMAN RIGHTS WATCH, *China: Police "Big Data" Systems Violate Privacy, Target Dissent. Automated Systems Track People Authorities Claim "Threatening"*, in www.hrw.org, 19 novembre 2017.

IASELLI M., *Algoritmi in ambito amministrativo, il Consiglio di Stato delinea i limiti*, in www.altalex.com, 20 gennaio 2020.

IEEE, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*, 2018, II versione, pp. 20-32.

ICO, *Big Data, artificial intelligence, machine learning and data protection*, 2017.

INTERPOL – UNICRI, *Artificial Intelligence and Robotics for Law Enforcement*, 2019.

INTERPOL – UNICRI, *Towards Responsible Artificial Intelligence Innovation*. *Second INTERPOL-UNICRI Report on Artificial Intelligence for Law Enforcement*, 2020.

ITALIANO G. F., *Intelligenza artificiale: passato, presente, futuro*, in F. PIZZETTI (a cura di) *Intelligenza artificiale, protezione dei dati personali e regolazione,* Giappichelli Editore, Torino 2018.

ITALIANO G.F., *Intelligenza artificiale, che errore lasciarla agli informatici*, in www.agendadigitale.eu, 11 giugno 2019.

KAPLAN J., *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press, II ed., 2018.

KENNEDY L.W. – DUGATO M., *Forecasting Crime and Understanding its Causes. Applying Risk Terrain Modeling Worldwide*, in *European Journal on Criminal Policy and Research*, vol. 24, n. 4/2018, pp. 345-513.

KOSTORIS R.E., *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella Risoluzione del XVIII Congresso internazionale di diritto penale*, in *Rivista di Diritto Processuale*, n. 2/2010, pp. 327 e ss.

KOSTORIS R.E., *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in F. RUGGIERI – L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità organizzata. Aspetti sostanziali e processuali*, Giappichelli Editore, Torino 2011, pp. 179 e ss.

KOSTORIS R.E., *Predizione decisoria,* diversion *processuale e archiviazione*, in www.sistemapenale.it, 23 luglio 2021.

KÖBIS N. – STARKE C. –RAHWAN I., *Artificial Intelligence as an Anti-Corruption Tool (AI-ACT). Potentials and Pitfalls for Top-down and Bottom-up Approaches*, in www.arxiv.org, Sez. *Computer Science > Computers and Society*, 23 febbraio 2021.

KOSSOW N. – DYKES V., *Blockchain, bitcoin and corruption. A review of the linkages*, in *Transparency International Anti-Corruption Helpdesk Answer*, 22 gennaio 2018.

KREMER J., *The End of Freedom in Public Places? Privacy problems arising from surveillance of the European public space*, 2017.

LANDOLFI M., *Le videoriprese investigative tra gli incerti confini giurisprudenziali e le crescenti esigenze di tutela della* privacy, in *Archivio penale*, n. 1/2022.

LASAGNI G., *L'uso di captatori informatici (*trojans*) nelle intercettazioni tra presenti*, in *Diritto Penale Contemporaneo*, 7 ottobre 2016.

LIMITI C., *Intelligenza Artificiale: implicazioni etiche in materia di privacy e diritto penale*, in www.iusinitinere.it, 9 febbraio 2021.

LIMITI C., *Corruzione: digitalizzazione e* open data, in www.iusinitinere.it, 16 marzo 2021.

LIU H. – LIN C. – CHEN Y., *Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability*, in *International Journal Of Law And Information Technology*, vol. 27, n. 2/2019, pp. 122-141.

LOMBARDO E., *Sicurezza 4P. Lo studio alla base del software XLAW per prevedere e prevenire i crimini*, Mazzanti Libri, Venezia 2019.

LOMBARDO E., *Intelligenza Artificiale e* human intelligence *per la prevenzione dei crimini*, Società italiana di Intelligence Press, 2020.

LÓPEZ-ITURRIAGA F.J. – PASTOR SANZ I., *Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces*, in *Social Indicators Research: An International and Interdisciplinary Journal for Quality-of-Life Measurement,* vol. 140**,** n. 3/2018, pp. 975-998.

LORUSSO S., Digital evidence*,* cybercrime *e giustizia penale 2.0*, in *Processo penale e giustizia*, 2019, pp. 821 e ss.

LUM K. – ISAAC W., *To predict and serve?*, in *Significance*, vol. 13, n. 5/2016, pp. 14-19.

LUND J., *New Legal Framework for Predictive Policing in Denmark,* in www.edri.org, 22 febbraio 2017.

LUPÁRIA L., *Prova giudiziaria e ragionamento artificiale: alcune possibili chiavi di lettura*, in J. SALLANTIN – J.-J. SZCZECINIARZ (a cura di), *Il concetto di prova alla luce dell'intelligenza artificiale*, Giuffrè Editore, Milano 2005.

LUPÁRIA L. – ZICCARDI G., *Investigazione penale e tecnologia informatica*, Giuffrè, Milano 2007.

MACCHIA M., *Blockchain e pubblica amministrazione*, in www.federalismi.it, n. 2/2021, pp. 117-129.

MACRÌ I., Open data, open format*: trasparenza e pubblicità dei dati delle Pubbliche Amministrazioni*, in *Azienditalia*, n. 8-9/2021, pp. 1431-1438.

MAGRO M.B., *Biorobotica, robotica e diritto penale*, in D. Provolo – S. Riondato – F. Yenisey (a cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, 2014.

MAGRO M.B., *Robot, cyborg e intelligenze artificiali*, in A. CADOPPI – S. CANESTRARI – A. MANNA – M. PAPA, *Cybercrime*, Utet Giuridica, Milano 2019, pp. 1179 ss.

MALDONATO L., *Algoritmi predittivi e discrezionalità del giudice: una nuova sfida per la giustizia penale*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2019, pp. 401-416.

MANES V., *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in www.discrimen.it, 15 maggio 2020.

MASTROBUONI G., *Crime is Terribly Revealing: Information Technology and Police Productivity*, in *Review of Economic Studies*, vol. 87, n. 6/2020, pp. 2727-2753.

MCCORDUCK P., *Storia dell'Intelligenza Artificiale. Gli uomini, le idee, le prospettive*, Franco Muzzio Editore, Padova 1987.

MCCARTHY J.– M. L. MINSKY – N. ROCHESTER – C. E. SHANNON, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, August 31, 1955, rieditato in AAAI, *AI Magazine*, vol. XXVII, n. 4, 2006, pp. 12-14.

MENDOLA M., *One Step Further in the "Surveillance Society": The Case of Predictive Policing*, Tech and Law Center, 17 ottobre 2016.

MINISTERO DELLO SVILUPPO ECONOMICO, *Strategia nazionale per l'intelligenza artificiale*, 2019.

MONTESQUIEU C., *Esprit des Lois*, 1798.

MONTRÉAL UNIVERSITY, *Montréal Declaration for a Responsible Development of Artificial Intelligence*, 2018.

MORABITO C., *La chiave del crimine*, in *Polizia Moderna*, luglio 2015.

MORELLI C., *Giustizia predittiva: il progetto (concreto) della Corte d'appello di Brescia*, in www.altalex.com, 8 aprile 2019.

MORELLI C., *Furti e rapine: a sventarli ci pensa l'intelligenza artificiale!*, in www.altalex.com, 6 maggio 2019.

MORELLI C., *Intelligenza artificiale, ecco lo statuto giuridico*, in www.altalex.com, 9 dicembre 2019.

MORELLI C., *L'Intelligenza artificiale entra in Corte di Cassazione*, in www.altalex.com, 18 ottobre 2021.

MORO P., *Biorobotica e diritti fondamentali. Problemi e limiti dell'intelligenza artificiale*, in D. PROVOLO – S. RIONDATO – F. YENISEY (a cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, 2014, pp. 517 e ss.

NEGRI D., *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Archivio Penale*, n. 1/2016.

NERI V., *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in *Urbanistica e appalti*, n. 5/2021, pp. 581-594.

NICOLICCHIA F., *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2018, p. 176-189.

NICOTRA I.A. – VARONE V., *L'algoritmo, intelligente ma non troppo*, in *Rivista AIC*, n. 4/2019, pp. 86-106.

NIEVA-FENOLL J., *Intelligenza artificiale e processo*, Giappichelli, Torino 2019.

NISCO A., *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*, in *Diritto penale contemporaneo*, n. 4/2021.

NOCERINO W., *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Prima parte)*, in *Studium Iuris*, n. 7-8/2020, pp. 821-827.

NOCERINO W., *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Seconda parte)*, in *Studium Iuris*, n. 9/2020, pp. 1020-1031.

NOCERINO W., *Il tramonto dei mezzi di ricerca della prova nell'era 2.0*, in *Diritto penale e processo*, n. 8/2021, pp. 1017-1030.

ODILLA F., *Bots against corruption: Exploring benefits and limitations of AI-based anti-corruption technology*, Digital Media, Machine Learning, and Corruption: How the Newest Technological Development Facilitate and Curb Corruption Practices Across the World, 2021.

OCSE, *Principles on Artificial Intelligence*, 2019.

OCSE, *Analytics for Integrity: Data-driven approaches for enhancing corruption and fraud risk assessments*, 2019.

OSCE, *Prevenzione e lotta alla corruzione attraverso la digitalizzazione e una maggiore trasparenza*, decisione n. 6/20, Tirana, 2020.

OSWALD M. – GRACE J. – URWIN S.– BARNES G., *Algorithmic risk assessment policing models: lessons from the Durham HART model and "Experimental" proportionality*, in *Information & Communications Technology Law*, vol. 27, n. 2/2018, pp. 223-250.

PAGALLO U., *The laws of Robots. Crimes, Contracts and Torts*, Springer, Dordrecht 2013.

PAGALLO U., *Algoritmi e conoscibilità*, in *Rivista di filosofia del diritto*, n. 1/2020, pp. 93-106.

PARLAMENTO EUROPEO – COMMISSIONE PER LE LIBERTÀ CIVILI, LA GIUSTIZIA E GLI AFFARI INTERNI, *Relazione sulle implicazioni dei* Big Data *per i diritti fondamentali:* privacy*, protezione dei dati, non discriminazione, sicurezza e attività di contrasto*, 2016/2225(INI), 20 febbraio 2017.

PARLAMENTO EUROPEO – COMMISSIONE PER LE LIBERTÀ CIVILI, LA GIUSTIZIA E GLI AFFARI INTERNI, *Legal frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, Marzo 2017.

PARODI C. – SELLAROLI V., *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo*, 2019, n. 6.

PARONA L., *"*Government by algorithm*": un contributo allo studio del ricorso all'intelligenza artificiale nell'esercizio di funzioni amministrative*, in *Giornale di diritto amministrativo*, n. 1/2021, pp. 10-18.

PASCULLI L., *Genetics, robotics and crime prevention*, in D. PROVOLO – S. RIONDATO – F. YENISEY (a cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, 2014, pp. 187 e ss.

PASQUALE F., *The Black Box Society: The Secret Algorithms that Control Money and Information*, Harvard University Press, Cambridge - London 2015.

PATRONI GRIFFI F., *La decisione robotica e il giudice amministrativo*, in A. CARLEO (a cura di), *Decisione robotica*, il Mulino, Bologna 2019, pp. 165-178.

PATRUNO V., *Il* Data & Analytics Framework *(Daf) è la Piattaforma Digitale Nazionale Dati: i punti chiave*, in www.agendadigitale.eu, 29 gennaio 2019.

PAULESU P.P., *La presunzione di non colpevolezza dell'imputato*, Giappichelli Editore, Torino 2009.

PEARSALL B., *Predictive Policing: The Future of Law Enforcement?*, in *NIJ Journal,* n. 266, 2010.

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.

PINELLI C., *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di Stato"*, in *Diritto Penale Contemporaneo*, fasc. n. 4/2017.

PISANI C. – PROIA G. – TOPO A. (a cura di), Privacy *e lavoro. circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Francis Lefebvre, Milano 2022.

PISATI M., *Indagini preliminari e intelligenza artificiale: efficienza e rischi per i diritti fondamentali*, in *Processo penale e giustizia*, fasc. n. 4/2020, pp. 957-971.

POLICE EXECUTIVE RESEARCH FORUM. 2014, *Future trends in policing*, Washington, D.C.: Office of Community Oriented Policing Services, 2014.

POLIDORO D., *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *Archivio penale*, n. 3/2020

PRESIDENZA DEL CONSIGLIO DEI MINISTRI – DIPARTIMENTO DELLA FUNZIONE PUBBLICA, *Linee Guida per la compilazione del Piano Integrato di Attività e Organizzazione (PIAO)*, circolare 6 dicembre 2021.

PROCACCINO A. – NOCERINO W., *Le nuove investigazioni nei reati corruttivi informatici*, in *Diritto penale e processo*, n. 12/2020, pp. 1623-1640.

QUATTROCOLO S., *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in www.lalegislazionepenale.eu, 18 dicembre 2018.

QUATTROCOLO S., *Equità del processo penale e* automated evidence *alla luce della Convenzione Europea dei Diritti dell'Uomo*, in *Revista italo-española de Derecho Procesal*, vol. 1, 2019, pp. 107-123.

QUATTROCOLO S., *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cassazione Penale*, n. 4/2019.

QUATTROCOLO S., *Artificial Intelligence, Computational modelling and Criminal Proceedings: A Framework for a European Legal Discussion*, Springer, 2020.

QUATTROCOLO S., *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in www.medialaws.eu (*Rivista di diritto dei media*), n. 3/2020, pp. 121-135.

RANALDI G., *Processo penale e prova informatica: profili introduttivi*, in *Diritto Pubblico Europeo Rassegna* online, n. 2/2020.

RICCIO G., *Ragionando su intelligenza artificiale e processo penale*, in *Archivio penale*, n. 3/2019.

RICHARDSON R. – SCHULTZ J. – CRAWFORD K., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, in *New York University Law Review Online*, vol. 94, n. 15/2019, pp. 192-233.

RIONDATO S., *Robot: Talune implicazioni di diritto penale*, in P. MORO – C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Franco Angeli Editore, Milano 2017, pp. 85-98.

ROVELLI M., *L'intelligenza artificiale in tribunale: dal giudice robot in Cina alle sperimentazioni in Italia*, in www.corriere.it, 3 marzo 2022.

RUFFOLO U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano 2020.

RUFFOLO U., Machina iuris-dicere potest*?*, in www.biodiritto.org, *BioLaw Journal – Rivista di BioDiritto*, n. 2/2021.

RUFFOLO U., *Giustizia predittiva e* machina sapiens *quale "ausiliario" del giudice umano*, in www.astrid-online.it, fasc. n. 8/2021.

SANTOSUOSSO A., *When the agent is not necessarily a human being, Some legal thoughts*, in D. PROVOLO – S. RIONDATO – F. YENISEY (a cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, 2014, pp. 545 e ss.

SANVITALE F., *A Milano la polizia ha KeyCrime, il software che prevede i reati. E funziona.*, in www.cronaca-nera.it, 9 aprile 2015.

SAVAZZI A.M. – CARDAMONE R., *Il Piano Integrato di Attività e Organizzazione (PIAO)*, in *Azienditalia*, n. 4/2022, pp. 775-784.

SCHAEFFER F., *En Chine, 1,4 milliard de suspects sous surveillance*, in www.lesechos.fr, 6 giugno 2018.

SCHANK R.C., *What's AI, Aniway?*, in AAAI, *AI Magazine*, vol. VIII, n. 4, 1987.

SEARLE J.R., *Menti, cervelli e programmi*, in D. R. HOFSTADTER – D. C. DENNETT (a cura di), *L'io della mente*, Adelphi, 1985, pp. 341-375.

SIGNORELLI A.D., *Il software italiano che ha cambiato il mondo della polizia predittiva*, in www.wired.it, 18 maggio 2019.

SIMONCINI A., *Diritto costituzionale e decisioni algoritmiche*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini, Pisa 2020, pp. 37-65.

SEVERINO P., *Intelligenza artificiale e diritto penale*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano 2020, pp. 531-545.

SEVERINO P., *Corruzione e crisi pandemica: vecchi problemi e nuove sfide*, in M. CATENACCI – V.N. D'ASCOLA – R. RAMPIONI, *Studi in onore di Antonio Fiorella. Volume II*, Roma Tr**E-Press**, Roma 2021, pp. 1879-1894.

SGUBBI F., *Il diritto penale totale. Punire senza legge, senza verità, senza colpa. Venti tesi*, il Mulino, Bologna 2019.

SIGNORATO S., *La localizzazione satellitare nel sistema degli atti investigativi*, in *Rivista italiana di diritto e procedura penale*, n. 2/2012, pp. 580-607.

SIGNORATO S., *Tipologie e caratteristiche delle* cyber investigations *in un mondo globalizzato*, in *Diritto Penale Contemporaneo*, fasc. n. 3/2016.

SIGNORATO S., *Modalità procedimentali dell'intercettazione tramite captatore informatico*, in G. GIOSTRA – R. ORLANDI (a cura di), *Nuove norme in tema di intercettazioni*, Giappichelli Editore, Torino 2018, pp. 263-275.

SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018.

SIGNORATO S., *Intercettazioni di comunicazioni*, in R. ORLANDI – S. SEMINARA (a cura di), *Una nuova legge contro la corruzione*, Giappichelli Editore, Torino 2019, pp. 245-260.

SIGNORATO S., *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo*, in *Rivista di Diritto Processuale*, n. 2/2020.

SIGNORATO S., *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, in *Rivista di diritto processuale*, vol. 76, n. 1/2021, pp. 101-110.

SIGNORATO S., *Rimodulazioni normative dell'uso investigativo del captatore informatico*, in R. ORLANDI – G. GIOSTRA (a cura di), *Revisioni normative in tema di intercettazioni. Riservatezza, garanzie difensive e nuove tecnologie informatiche*, Giappichelli Editore, Torino 2021, pp. 319-335.

SIRACUSANO D., *Dal processo inquisitorio al processo accusatorio. Luci ed ombre di una svolta epocale*, Torino 25 luglio 2013.

SMUHA N.A., *The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence*, in *Computer Law Review International*, vol. 20, n. 4/2019, pp. 97-106.

SPRICK D., *Predictive Policing in China: An Authoritarian Dream of Public Security*, in *Naveiñ Reet: Nordic Journal of Law and Social Research (NNJLSR),* n. 9/2019, pp. 299-324.

STANFORD UNIVERSITY, *Artificial Intelligence and Life in 2030. One Hundred year study on Artificial Intelligence*, 2016.

SUSIO B. – BARBAGALLO E., *Dal PTPCT al PIAO: la strategia di prevenzione della corruzione fa sinergia e si rafforza*, in *Azienditalia*, n. 4/2022, pp. 699-706.

TACITO P.C., *Annales*, Libro III, par. 27.

THOMAS E., *Why Oakland Police Turned Down Predictive Policing*, in www.vice.com, 28 dicembre 2016.

THOMPSON C., *Myths and Facts: Using Risk and Need Assessments to Enhance Outcomes and Reduce Disparities in the Criminal Justice System*, NIC, marzo 2017.

TORRE M., *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Diritto penale e processo*, n. 8/2021, pp. 1042-1056.

TRAVERSI A., *Intelligenza artificiale applicata alla giustizia: ci sarà un giudice* robot*?*, in www.questionegiustizia.it, 10 aprile 2019.

TRESCA M., *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia digitale*, in www.medialaws.eu (*Rivista di diritto dei media*), n. 3/2018, pp. 240-252.

TRIPODI E.M., *Decisioni automatizzate nella PA: i dieci principi indicati dalla giurisprudenza*, in www.agendadigitale.eu, 12 ottobre 2021.

TURING A. M., *Calcolatori e intelligenza*, in D. R. HOFSTADTER – D. C. DENNETT (a cura di), *L'io della mente*, Adelphi, 1985, pp. 61-100.

UBERTIS G., *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto Penale Contemporaneo*, fasc. n. 4/2020, pp. 75-88.

VENTURI M., *KeyCrime©. La chiave del crimine*, in *Profiling. I profili dell'abuso*, n. 4/2014.

VILLANI C., *For a Meaningful Artificial Intelligence*, 2018.

VIOLA L., *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in www.federalismi.it, n. 21/2018.

VIOLA L. (a cura di), *Giustizia predittiva e interpretazione della legge con modelli matematici. Atti del Convegno tenutosi presso l'Istituto dell'enciclopedia Italiana Treccani*, Diritto Avanzato, Milano 2019.

VIOLA L., *Giustizia predittiva: è preferibile un modello deduttivo*, in www.altalex.com, 10 marzo 2020.

ZAVRŠNIK A. (a cura di), *Big Data, crime and social control*, Routledge – Taylor & Francis Group, 2018.

ZIROLDI A., *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in www.questionegiustizia.it, 18 ottobre 2019.

ZUBOFF S., *Il capitalismo della sorveglianza*, Luiss University Press, Roma 2019.