CONVEGNI

BENEDETTA GALGANI

Giudizio penale, *habeas data* e garanzie fondamentali*

La recente *policy* europea in materia di salvaguardia del diritto all'autodeterminazione informativa rappresenta l'occasione per interrogarsi, più in generale, sulla tenuta dei diritti fondamentali, non soltanto nello spettro del processo penale, ma altresì al cospetto di un apparato preventivo sempre più "in espansione". Muovendo dai contenuti della Direttiva 2016/680/UE, in un raffronto peraltro costante con la disciplina di attuazione interna all'ordinamento italiano, l'analisi si appunta su talune tematiche centrali quali il rispetto del principio di proporzionalità, della presunzione di non colpevolezza e dei canoni decisori classici a fronte dell'impiego delle nuove tecnologie e dei sistemi di IA nell'ambito della giustizia penale.

The latest European policy concerning the right of informational self-determination provides an opportunity to reflect, in principle, about the protection of fundamentals rights, not only on the spectrum of criminal proceedings, but also in regard to the ever-expanding disciplines on preventive and security measures. Starting from the Directive 2016/680/UE, examined in an ongoing comparison with the italian domestic implementation, this work explores a few relevant issues, concerning the compliance to the principle of proportionality, the presumption of innocence and the traditional judgment's criteria with reference to the use of new technologies and the AI in the context of criminal justice

1. Scelta e contesto

La selezione di un tema aleatorio come quello che si è tentato di condensare sotto un titolo così ambizioso è il frutto di una scelta "di pancia", forse nemmeno del tutto consapevole.

È il frutto, in termini se si vuole un po' più aulici, di una sorta di *Inversionsmethode*: al cospetto, infatti, della sempre più imponente dimensione assunta dal fenomeno dell'evoluzione tecnologica[1] e dalla vera e propria metamorfosi che l'accelerazione dei suoi progressi sta imponendo alle nostre società democratiche, si è avvertita come non ulteriormente procrastinabile la necessità

*Testo rivisto, ampliato ed aggiornato ai più recenti provvedimenti normativi, dell'intervento svolto in seno al *Congreso Internacional "Confronto: Diálogo hispano-italiano sobre proceso penal",* che si è tenuto presso *la Facultad de Derecho de la Universidad de Cádiz* nei giorni 8-9 novembre 2018.

[1] Con il consueto nitore poetico, negli anni Ottanta CALVINO, (*Leggerezza*, in *Lezioni americane*, Milano 1988, 10) riconosceva che «la seconda rivoluzione industriale non si presenta come la prima con immagini schiaccianti quali presse di laminatoi o colate d'acciaio, ma con i bits d'un flusso d'informazione che corre sui circuiti sotto forma d'impulsi elettronici. Le macchine di ferro ci sono sempre, ma obbediscono ai bits senza peso».

di esaminare le più recenti politiche di "gestione" di tale complessità e di verificarne la tenuta in punto di difesa dei diritti e delle libertà fondamentali. Il tutto, come si vedrà, dal peculiare angolo visuale dei soggetti (anche soltanto occasionalmente) coinvolti dalle multiformi vicende dell'accertamento penale.

Lo stimolo più immediato a questa indagine è stato offerto dalla recente entrata in vigore di un articolato "pacchetto" di norme – di fonte sia eurounitaria che nazionale – volte ad ampliare ed approfondire la tutela dei dati personali.

Più in dettaglio, s'intende far riferimento al Regolamento 2016/679/UE "relativo alla protezione dei dati delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati personali)[2], entrato in vigore il 25 maggio 2018; alla Direttiva 2016/680/UE "relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI, il cui termine di recepimento era fissato per il 6 maggio 2018; al decreto legislativo 18 maggio 2018, n. 51, in vigore dall'8 giugno 2018, con cui il legislatore italiano ha dato attuazione alla citata Direttiva e, *last but not least*, al d.lgs. 10 agosto 2018, n. 101, entrato in vigore il 19 settembre scorso, con cui lo stesso legislatore ha modificato il Codice in materia di protezione dei dati personali (comunemente detto Codice della privacy: d.lgs. 196/2003) per adeguarne il contenuto al già vigente GDPR.

Ebbene, già ad un primissimo sguardo, il corposo *puzzle* normativo[3] che si è venuto costituendo in un così ristretto arco di tempo non sembra agevolare una lettura, per così dire, di "sistema": basti por mente alla circostanza per cui, sebbene il GDPR "incarni" la disciplina primaria e principale in materia, per l'appunto non necessitante di alcun atto legislativo di recepimento nazionale giacché contenuta in un regolamento comunitario di diretta applicazione, il "nuovo" Codice della Privacy conserva un ruolo niente affatto secondario, anche e soprattutto relativamente a quell'attività di specificazione e di integrazione dei principi generali che il GDPR ha rimesso ai singoli ordinamenti nazionali[4].

---

[2] ...cui di qui in avanti si farà riferimento con l'acronimo inglese GDPR (*General Data Protection Rules*).

[3] Parla di «elefantiaca normativa» ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Riv. dir. dei media* 2018, 2, 4.

[4] Tra l'altro, il legislatore italiano ha deciso di avvalersi di quasi tutte le cosiddette "clausole di apertura"

Ma, al di là delle censure che pure si potrebbero muovere alle scelte in punto di *drafting* legislativo adottate a livello domestico ove, come appena ricordato, si è preferito novellare ed interpolare un testo normativo già esistente, piuttosto che scriverne uno completamente nuovo alla luce del nuovo orizzonte sovranazionale[5], un assunto incontestabile è che – nella precipua prospettiva d'analisi qui prescelta, ossia quella della salvaguardia dei diritti individuali fondamentali nei confronti di un qualsiasi trattamento (non automatizzato, parzialmente automatizzato o interamente automatizzato) effettuato in ambito penale – tanto i due provvedimenti di rango europeo, quanto i due decreti legislativi di derivazione interna debbono essere letti in un'ottica di complementarietà integrata[6].

---

del GDPR, ossia di quelle disposizioni del Regolamento che consentono agli Stati membri di mantenere o introdurre norme specifiche ulteriori per la protezione dei dati personali. Più in particolare, si è sfruttata la facoltà di prevedere sanzioni penali (che vanno ad aggiungersi a quelle amministrative già previste dal Regolamento) per alcune violazioni della normativa sulla *privacy*. Rileva come i draconiani interventi infine operati sull'impianto sanzionatorio penale dal d.lgs. 101/2018 siano del tutto in controtendenza rispetto a quella che era la scelta originaria del legislatore delegato DEL NINNO, *Il decreto legislativo 101/2018 di modifica e coordinamento del Codice della Privacy al GDPR: uno sguardo di insieme sul nuovo quadro normativo nazionale sulla tutela dei dati personali*, in *www.dirittpegiustizia.it*.

[5] ... tanto più che, come la stessa Relazione illustrativa al d.lgs. 101/2018 espressamente dichiara, «codice e regolamento sono informati a due filosofie diverse» (*www.documenti.camera.it*). Se ne dovrebbe ricavare che la logica sottesa ad un'opzione di tal fatta sia quella efficacemente fotografata da Ennio Flaiano, a detta del quale «in Italia [...] la linea più breve tra due punti è l'arabesco».

[6] In questo senso basti vedere il *Considerando* n. 19 GDPR («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 contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati sono oggetto di uno specifico atto dell'Unione. Il presente regolamento non dovrebbe pertanto applicarsi ai trattamenti effettuati per tali finalità. I dati personali trattati dalle autorità pubbliche in forza del presente regolamento, quando utilizzati per tali finalità, dovrebbero invece essere disciplinati da un più specifico atto dell'Unione, segnatamente la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio») e il *Considerando* n. 11 Direttiva 2016/680/UE («È pertanto opportuno per i settori in questione che una direttiva stabilisca le norme specifiche relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, nel rispetto della natura specifica di tali attività. Tali autorità competenti possono includere non solo autorità pubbliche quali le autorità giudiziarie, la polizia o altre autorità incaricate dell'applicazione della legge, ma anche qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici ai fini della presente direttiva. Qualora tale organismo o entità trattino dati personali per finalità diverse da quelle della presente direttiva, si applica il regolamento (UE) 2016/679. Il regolamento (UE) 2016/679 si applica pertanto nei casi in cui un organismo o un'entità raccolgano dati personali per finalità diverse e procedano a un loro ulteriore trattamento per adempiere un obbligo legale cui sono soggetti»). Sul fronte interno, è invece sufficiente leggere l'art. 2-*opties* (*Principi relativi al trattamento di dati relativi a condanne penali e reati*) del Codice Privacy come novellato dal d.lgs. 101/2018 per apprezzare la complementarietà di cui si va disquisendo. Nel dettagliare i principi relativi al trattamento di dati relativi a condanne penali e reati (gli *ex* "dati giudiziari"), e nello stabilire che il trattamento che avviene al di

Di certo, il nucleo valoriale di ogni riflessione che di qui si dipanerà non può che essere quello prepotentemente posto in evidenza dal Trattato di Lisbona, ossia la legittimazione ad una tutela tanto autonoma quanto intensa del diritto alla protezione dei dati personali. Diversamente dall'interesse a lungo registrato per una tutela dei dati personali meramente strumentale ad assicurare una loro libera circolazione all'interno della Comunità Economica Europea, sia l'art. 8 § 1 della Carta dei Diritti dell'Unione che l'art. 16 del Trattato sul Funzionamento dell'Unione tutelano il diritto alla protezione dei dati personali *ex se*, facendolo finalmente assurgere a diritto fondamentale di ogni soggetto fisico residente nell'Unione[7]. E da una visione così profondamente rinnovata della protezione delle persone in riferimento al trattamento dei dati di carattere personale – visione che, *per incidens*, risultava tra l'altro debitrice della vivificante giurisprudenza delle Corti di Strasburgo[8] e di Lussemburgo[9] – doveva di necessità discendere anche una più matura consapevolezza circa l'urgenza che «la libera circolazione dei dati personali tra le autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, inclusi la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, all'interno dell'Unione e il trasferimento di tali dati personali verso paesi terzi e organizzazioni internazionali» dovesse «essere agevolata » attraverso «la costruzione di un quadro giuridico so-

---

fuori del controllo dell'autorità pubblica è lecito soltanto se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, ammettendo altresì, in via del tutto residuale, che detti trattamenti e le relative garanzie possano essere previsti da un decreto del Ministero della Giustizia, il testo della disposizione fa «salvo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51», ovvero, appunto, tutto ciò che concerne il trattamento dei dati personali da parte delle autorità competenti in materia penale così come disegnato dalla Direttiva 2016/680/UE.

[7] Cfr. BALSAMO, *Il contenuto dei diritti fondamentali*, in *Manuale di procedura penale europea*, a cura di Kostoris, Milano 2017, 169-170; PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino 2018, 5 ss. e PIETROPAOLI, Privacy *e diritto all'oblio. La protezione giuridica dei dati personali*, in FAINI PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, Torino 2017, 47-48. Per un esaustivo *excursus* storico sulla progressiva affermazione ed evoluzione, a livello di fonti e di giurisprudenze europee, dell'*habeas data*, cfr. PREZ-LUÑO ROBLEDO, *El procedimiento de* habeas data, Madrid 2017, 221 ss.

[8] Vd., *ex plurimis*, C.eur. 26.3.1987, *Leander* c. *Svezia* e C.eur. 26.2.2015, *Zaichenko* c. *Ucraina*; in dottrina, tra gli altri, Tomasi, *sub* art. 8, in *Commentario breve alla Convenzione europea dei diritti dell'uomo*, a cura di Bartole, De Sena, Zagrebelsky, Padova 2011, 315 ss.; GALLUCCIO, *Profili specifici sull'art. 8*, in *Corte di Strasburgo e giustizia penale*, a cura di Ubertis, Viganò, Torino 2016, 276.

[9] Vd., tra le pronunce più significative, Corte giust., 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland and Others*; Corte giust., 13.5.2014, C-131/12, *Google Spain e Google Inc. c. Agencia Espanõla de Protección de Datos e Mario Costeja González*; in dottrina, sullo «statuto giurisprudenziale della privacy digitale» vd. per tutti POLLICINO, BASSANI, *La Carta dei diritti fondamentali dell'Unione europea nel* reasoning *dei giudici di Lussemburgo*, in *La protezione transnazionale dei dati personali. Dai "*Safe Harbours Principles *" al "*Privacy Shield *"*, a cura di Resta, Zeno, Zencovich, Roma 2016, 73 ss.

lido e più coerente in materia di protezione dei dati personali nell'Unione, affiancato da efficaci misure di attuazione»[10] .

Il contrassegno di un'affinata sensibilità nei riguardi dei canoni che devono presiedere alla tutela dei dati personali (anche) quando i titolari del trattamento risultino le autorità giudiziarie e di polizia può rinvenirsi, anzitutto, nella maggior latitudine operativa della Direttiva 2016/680 rispetto a quella a suo tempo ascritta alla sua «antesignana»[11], vale a dire alla Decisione Quadro 2008/977/GAI[12]. Mentre quest'ultima si limitava a disciplinare la protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia, la Direttiva, per l'appunto abrogativa del provvedimento pre-Lisbona, si interessa non soltanto allo scambio transfrontaliero di dati personali, ma anche al trattamento che di essi venga effettuato all'interno di ciascun ordinamento nazionale da parte delle autorità giudiziarie, di polizia o comunque legittimate ad esercitare pubblici poteri[13].

---

[10] Cfr. *Considerando* n. 4 Direttiva 2016/680/UE. *Per incidens*, che l'interesse prioritario dell'Unione sia stato (e, in parte, tutt'oggi continui ad essere) il miglioramento della cooperazione giudiziaria in chiave repressiva e preventiva non è argomento suscettibile di smentita.

[11] Così, testualmente, BORGIA, *Il trattamento di dati personali ai fini di prevenzione, di indagine, di accertamento e di perseguimento di reati o di esecuzione di sanzioni penali: quali passi avanti alla luce dei recenti sviluppi?*, in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di Mantelero, Poletti, Pisa 2018, formato *e-book*, 497, al cui contributo si rimanda anche per un'attenta sintesi delle altre criticità palesate dal previgente testo eurounitario nei confronti di una tutela che potesse dirsi davvero effettiva del diritto all'autodeterminazione informativa.

[12] Cfr. per tutti DI PAOLO, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in *Cass. pen.* 2010, 1978 e BAZZOCCHI, *La decisione quadro sulla protezione dei dati personali nel terzo pilastro*, reperibile all'indirizzo *www.europeanrights.eu*.

[13] Concordemente SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino 2018, 86-87; PULITO, *Il trattamento dei dati personali in ambito penale e l'uso del* passenger name record *per contrastare il terrorismo e altri gravi reati*, in *Processo Penale e Giustizia* 2018, 6, 1140; e BORGIA, *Il trattamento di dati personali ai fini di prevenzione, di indagine, di accertamento e di perseguimento di reati o di esecuzione di sanzioni penali: quali passi avanti alla luce dei recenti sviluppi?*, cit., 499 ss.; per converso, ritiene che anche la Direttiva 2016/680 limiti il suo ambito d'intervento al solo settore della cooperazione giudiziaria in materia penale SORRENTINO, *Il controllo del garante per la protezione dei dati personali e l'autorità giudiziaria secondo le più recenti norme eurounitarie*, in *www.questionigiustizia.it*.

Piuttosto, proprio con specifico riferimento al settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, la Direttiva *de qua* è stata eletta ad "architrave" normativa di riferimento per il trattamento e l'accesso ai dati inseriti nel sistema d'informazione Schengen (SIS) ad opera del *Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio* adottato il 28.11.2018 (per il testo si veda all'indirizzo *eur-lex.europa.eu*). Così come recita, infatti, il *Considerando* n. 21, la possibilità delle autorità nazionali competenti di consultarlo in conformità ai principi stabiliti nella Direttiva 2016/680, dovrebbe «permettere al SIS di funzionare come principale misura compensativa nello spazio senza controlli alle frontiere interne e di contrastare meglio la dimensione transfrontaliera della criminalità e la mobilità dei criminali».

Non soltanto: seppure rimasta *ab initio* nell'ombra a causa della straordinaria risonanza (anche mediatica) che ha accompagnato l'adozione del Regolamento, chiamato a rendere per la prima volta davvero uniforme – per non dire unica – in tutti i Paesi dell'Unione la normativa in materia di protezione dei dati a carattere personale, la Direttiva 680/2016/UE vanta finalità ed obiettivi non meno nobili, attuali e rilevanti.

Va da sé che, proprio in forza del "corredo cromosomico" che la contraddistingue, di atto cioè non immediatamente applicabile, essa affidi gran parte della sua *vis* armonizzatrice alle modalità attuative dei singoli ordinamenti e, pur sostanzialmente riproducendo i principi garantistici consacrati nel GDPR anche e soprattutto in tema di diritti dell'interessato e doveri del titolare, ne tolleri (più o meno evidenti) compressioni in nome di specifici interessi relativi alla sicurezza pubblica da un lato, e all'esercizio dell'attività giudiziaria dall'altro. Ciò che in definitiva non sorprende è che, nell'atto dell'Unione precipuamente dedicato agli impieghi delle informazioni di natura personale a fini di giustizia penale, la necessità di contemperamento tra interessi diversamente rilevanti possa emergere semmai più evidente di quanto pure non avvenga in seno al regolamento europeo, in apertura del quale, ad ogni buon conto, il legislatore dell'Unione si preoccupa di evidenziare che «il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta», bensì «va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità» (*Considerando* n. 4)[14].

Parallelamente, quasi a voler ricordare che – mutuando l'icastica espressione utilizzata dal nostro Giudice delle Leggi in occasione di una delle pronunce sul c.d. "caso Ilva" – nessun diritto, per quanto fondamentale, è «tiranno»[15], anche il legislatore della Direttiva si sofferma in via di premesse sugli interventi limitativi che potranno essere apposti a taluni dei diritti individuali ivi enunciati. In quest'ottica, a fronte di un prezioso e dettagliato riconoscimento del diritto ad ottenere informazioni, del diritto di accesso, del diritto di rettifica e, ancora, del diritto di cancellazione e di limitazione al trattamento riconosciuti

[14] Cfr. altresì PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., 39.

[15] Cfr. Corte cost., n. 85 del 2013, reperibile all'indirizzo *www.cortecostituzionale.it, il cui § 9 del Considerato in diritto così recita: «*Tutti i diritti fondamentali tutelati dalla Costituzione si trovano in rapporto di integrazione reciproca e non è possibile pertanto individuare uno di essi che abbia la prevalenza assoluta sugli altri. La tutela deve essere sempre "sistemica e non frazionata in una serie di norme non coordinate ed in potenziale conflitto tra loro" (sentenza n. 264 del 2012). Se così non fosse, si verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe "tiranno" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette, che costituiscono, nel loro insieme, espressione della dignità della persona».

in capo al titolare dei dati, il testo europeo non tralascia di legittimare gli Stati membri ad «adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato o a limitare, in tutto o in parte, l'accesso di questi ai suoi dati personali nella misura e per la durata in cui ciò costituisca una misura necessaria e proporzionata in una società democratica [...] per non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento dei reati o l'esecuzione di sanzioni penali, per proteggere la sicurezza pubblica o la sicurezza nazionale o per tutelare i diritti e le libertà altrui» (*Considerando* n. 44).

Dunque, inserendosi in un filone interpretativo in via di costante consolidamento, anche il secondo dei provvedimenti "manifesto" della *policy* europea in tema di salvaguardia del diritto all'autodeterminazione informativa, dimostra un approccio più maturo al binomio *privacy-sicurezza* come tradizionalmente inteso. Più in particolare, facendo perno sul richiamo espresso a quello che ormai può dirsi assurto a paradigma generale di valutazione in punto di legittimità delle incursioni delle autorità statali nel "bagaglio" garantistico dei singoli[16], il legislatore della Direttiva si sforza di delineare e di additare agli ordinamenti dei Paesi che ad essa dovranno adeguarsi una composizione "proporzionata" tra le *chances* in astratto accordabili al potere giudiziario e di polizia, di conoscere e trattare «praterie di dati personali»[17] in nome di un accertamento giurisdizionale e di un sistema di prevenzione il più possibile efficienti, e la salvaguardia delle libertà individuali dei comuni cittadini che si tro-

[16] Alla progressiva affermazione del canone ermeneutico della proporzionalità quale principio chiave del diritto europeo hanno senz'altro contribuito, da una parte, la lettera dell'art. 52 della Carta dei Diritti Fondamentali dell'Unione Europea e, dall'altra, una ricca giurisprudenza della Corte di Strasburgo che, anche e soprattutto con riferimento ai *vulnera* arrecati alla vita privata dei singoli per mezzo di strumenti di controllo particolarmente subdoli ed invasivi, ha costantemente lavorato per "mettere a fuoco" i caratteri strutturali del medesimo: nella copiosa letteratura, per quanto specificamente attiene alla "riscoperta" del principio *de quo* nel diritto processuale penale, cfr. CAIANIELLO, *Il principio di proporzionalità nel processo penale*, in *Riv. trim. diritto penale cont.,* 2014, 3-4; 143 ss; DANIELE, *I chiaroscuri dell'OEI e la bussola della proporzionalità*, in *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, a cura di Daniele, Kostoris), Torino 2018, 55 ss.; KOSTORIS, *Processo penale e paradigmi europei*, Torino 2018, 141-142; FALATO, *La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale*, in *questa Rivista*; NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *www.penalecontemporaneo.it*, e, con specifica attenzione alle letture "deformanti" che dello stesso principio sono state adottate a livello di giurisprudenza interna, UBERTIS, *Equità e proporzionalità* versus *legalità processuale: eterogenesi dei fini?*, in *questa Rivista*.

[17] L'espressione, plastica, è presa in prestito da GIOSTRA, *I nuovi equilibri tra diritto alla riservatezza e diritto di cronaca nella riformata disciplina delle intercettazioni*, in *Riv. it. dir. proc. pen.*, 2018, 2, 521 ss. ed è volta a sottolineare che le fonti dalle quali i dati personali possono provenire sono indefinite e sostanzialmente infinite.

vino variamente coinvolti nei multiformi meccanismi di indagine e di definizione di una vicenda penale. Non sempre riuscendoci. Difatti, complice «la natura intrinsecamente discrezionale del giudizio di bilanciamento tra valori»[18] su cui lo scrutinio di proporzionalità – che per l'appunto dovrebbe presiedere a qualunque scelta politico normativa – essenzialmente si fonda; complice, altresì, la straordinaria rapidità con cui la tecnologia compie i suoi progressi ponendo di continuo l'operatore del diritto dinanzi a fenomeni del tutto inediti la cui unica possibilità di "governo" sembra rimessa all'adozione di clausole aperte o comunque a formulazione indeterminata[19], non tutti i risultati infine tradotti nell'atto normativo di riferimento possono essere reputati del tutto soddisfacenti.

2. Tre questioni "critiche". Diritto alla cancellazione e *data retention...*

Premesso che in questa sede non avrebbe senso procedere ad una rassegna analitica dei contenuti della Direttiva e della normativa italiana con cui a quella si è inteso dare attuazione, onde conferire maggiore spessore a quanto fin qui osservato e poter saggiare, quindi, la "solidità" in punto di garanzie dell'assetto giuridico complessivamente approntato, sarà sufficiente puntare la "lente d'ingrandimento" su alcuni dei profili presi in esame dalla legislazione eurounitaria.

Il primo tema attinge specificamente il diritto alla cancellazione dei dati personali. Quest'ultimo – declinazione ulteriore di quel principio di proporzionalità che, così come declamato nell'art. 4 § 1 lettere *e)* della Direttiva 2016/680, dovrebbe caratterizzare anche i tempi di conservazione dei dati personali oggetto di trattamento – consta, tra l'altro, dell'obbligo in capo agli Stati e di fissare «adeguati termini per la cancellazione dei dati personali» (art. 5 della Direttiva 2016/680), e di imporre «al titolare del trattamento di cancellare i dati personali senza ingiustificato ritardo» (art. 16 § 2 della Direttiva 2016/680).

Orbene, a destare subitanee perplessità sono proprio i vocaboli ed i lemmi appena richiamati («adeguati», «senza ingiustificato ritardo») giacché non è certo un impiego, quand'anche ricco e ridondante, di una certa aggettivazione che può contenere gli abusi, anzi...

---

[18] NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, cit.

[19] Del resto, lo stesso GDPR, i cui lavori preparatori erano cominciati nel 2010, vale a dire subito dopo l'entrata in vigore del Trattato di Lisbona, rischiava e rischia di risultare già superato dall'evoluzione della tecnologia che per l'appunto rende possibili pratiche di trattamento e di raccolta sempre nuove: in questi termini cfr. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, 5 ss.

Di fatto, le previsioni eurounitarie risultano a tal punto vaghe ed indeterminate da lasciare ai singoli ordinamenti un margine di manovra molto ampio, sicuramente distonico rispetto all'intento armonizzatore, nell'ambito del quale il (presunto) equilibrio tra tutela dei dati e loro impiego a fini di giustizia può assumere fisionomie le più diverse e discutibili, facendo (anche) del proclamato diritto alla cancellazione un "guscio" carente della sua essenza assiologica.

A confermare questi dubbi contribuisce, laddove ve ne fosse bisogno, la normativa interna. Il decreto legislativo 51/2018 – che con un non trascurabile tasso di ambizione si riproponeva, come documentato dalla stessa Relazione illustrativa, di «creare un vero e proprio statuto sulla raccolta e il trattamento dei dati personali in ambito penale»[20] – si è invece limitato a replicare pressoché pedissequamente gli enunciati del provvedimento europeo: «i dati personali», recita l'art. 3, co. 1, sono «conservati [...] per il tempo necessario al conseguimento delle finalità per le quali sono trattati, sottoposti ad esame periodico per verificarne la persistente necessità di conservazione, cancellati [...] una volta decorso tale termine» e, giusta la lettera dell'art. 12, co. 2, il titolare del trattamento deve procedere alla loro cancellazione «senza ingiustificato ritardo [...] in ogni altro caso previsto dalla legge».

Ma qual è, dunque e in concreto, il lasso di tempo entro il quale la conservazione di dati personali acquisiti per finalità di prevenzione e di repressione penale può dirsi (ancora) "necessaria" ed il correlato termine di cancellazione "non inadeguato"? Com'è evidente, la risposta a questo interrogativo deve essere cercata altrove. Precisamente in un decreto del Presidente della Repubblica, il n. 15 del 15 gennaio 2018, che, in ottemperanza all'art. 57 del Codice della privacy nella sua versione originaria, individuava e (tuttora) individua la disciplina di dettaglio in relazione, appunto, al trattamento dei dati effettuato esclusivamente per finalità di polizia giudiziaria e di tutela dell'ordine e della sicurezza pubblica.

Al di là dell'iniziale "smarrimento" indotto dal constatato ricorso ad un provvedimento di rango non legislativo[21], per di più entrato in vigore sotto l'egida di una fonte primaria comunque "altra" rispetto a quella che di lì a poco sa-

[20] Il testo è reperibile all'indirizzo *documenti.camera.it*.

[21] Su questo sempre più frequente passaggio di poteri dal legislativo all'esecutivo, aveva già avuto modo di riflettere SIGNORATO, *Il trattamento dei dati personali per le finalità di polizia: la nuova disciplina prevista dall'art. 53 Codice Privacy e gli scenari europei*, in *Il nuovo "pacchetto" antiterrorismo,* a cura di Kostoris, Viganò, Torino 2015, 95-96, ascrivendone la causa all'esigenza di rapidità nell'adozione di provvedimenti volti a regolare una materia in troppo rapido divenire per le tempistiche parlamentari.

rebbe sopravvenuta[22], ciò su cui merita soffermare l'attenzione è il dettato dell'art. 10 del decreto: i termini di conservazione dei dati vanno dai 18 mesi ai 30 anni, e possono essere ulteriormente aumentati, per un periodo non superiore ai 2/3 del periodo iniziale, quando i dati siano trattati per attività relative ai delitti di cui agli artt. 51 co. 3-*bis, 3-quater* e 3-*quinquies*, all'art. 407, co. 2 lett. *a)* c.p.p. (co. 3), nonché, ancora, quando lo decida il comandante del reparto, in base alle linee guida indicate dal Capo della Polizia ex art. 4, co. 6, legge 410/1991, segnalando i motivi in relazione al caso specifico (co. 5).

Ebbene, già da questa generica ricognizione, si fa fatica a considerare delle tempistiche così significativamente prolungate di *data retention* in linea con un contesto europeo che, almeno in via di enunciati ed al netto delle precisazioni e delle cautele che pure si sono rammentate, si dimostra sempre più sensibile ed attento ad enucleare le modulazioni del diritto alla protezione dei

[22] La "riconduzione all'ordine" è stata cautelativamente rimessa alle motivazioni elencate al Capo I (Disposizioni generali), ove il regolamento rinvia comunque a tutta una serie di normative internazionali e dell'Unione Europea, tra le quali campeggiano anche il GDPR e la Direttiva i cui termini di entrata in vigore, al momento dell'approvazione, erano per l'appunto ormai prossimi.
Più in dettaglio, l'art. 57 Codice della Privacy (il cui testo recita: «1. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro della giustizia, sono individuate le modalita' di attuazione dei principi del presente codice relativamente al trattamento dei dati effettuato per le finalità di cui all'articolo 53 dal Centro elaborazioni dati e da organi, uffici o comandi di polizia, anche ad integrazione e modifica del decreto del Presidente della Repubblica 3 maggio 1982, n. 378, e in attuazione della Raccomandazione R (87) 15 del Consiglio d'Europa del 17 settembre 1987, e successive modificazioni. Le modalità sono individuate con particolare riguardo:
a) al principio secondo cui la raccolta dei dati e' correlata alla specifica finalità perseguita, in relazione alla prevenzione di un pericolo concreto o alla repressione di reati, in particolare per quanto riguarda i trattamenti effettuati per finalità di analisi;
b) all'aggiornamento periodico dei dati, anche relativi a valutazioni effettuate in base alla legge, alle diverse modalità relative ai dati trattati senza l'ausilio di strumenti elettronici e alle modalità per rendere conoscibili gli aggiornamenti da parte di altri organi e uffici cui i dati sono stati in precedenza comunicati;
c) ai presupposti per effettuare trattamenti per esigenze temporanee o collegati a situazioni particolari, anche ai fini della verifica dei requisiti dei dati ai sensi dell'articolo 11, dell'individuazione delle categorie di interessati e della conservazione separata da altri dati che non richiedono il loro utilizzo;
d) all'individuazione di specifici termini di conservazione dei dati in relazione alla natura dei dati o agli strumenti utilizzati per il loro trattamento, nonché alla tipologia dei procedimenti nell'ambito dei quali essi sono trattati o i provvedimenti sono adottati;
e) alla comunicazione ad altri soggetti, anche all'estero o per l'esercizio di un diritto o di un interesse legittimo, e alla loro diffusione, ove necessaria in conformità alla legge;
f) all'uso di particolari tecniche di elaborazione e di ricerca delle informazioni, anche mediante il ricorso a sistemi di indice») sarà abrogato decorso un anno dall'entrata in vigore del d.lgs. 51/2018, secondo quanto stabilito dall'art. 49, co. 2 del medesimo. Diversamente, gli artt. 53-56 dello stesso Codice, sono stati immediatamente abrogati dal primo comma dell'art. 49 d.lgs. 51/2018.

dati come espressione, in definitiva, dell'identità personale del soggetto[23].
Provando quindi a calare il discorso nella "materialità" di alcune fattispecie modulate dalla disposizione dell'atto regolamentare, può davvero ritenersi conforme al principio di proporzionalità la conservazione di «dati relativi ad attività di polizia giudiziaria conclusa con provvedimento di archiviazione» per «20 anni dall'emissione del provvedimento» (lett. *f*)? O, ancora ed addirittura, la conservazione per 15 anni dall'ultimo trattamento di quei dati che non abbiano neppure «dato luogo a procedimento penale»?
L'intonazione enfaticamente retorica di queste domande tradisce – è evidente – un giudizio negativo che, tuttavia, non sembra trovare smentita nemmeno nelle sorti di altre (e non meno preoccupanti) scelte politiche compiute di recente dal nostro ordinamento: si pensi, in particolare, all'art. 24 della Legge Europea 2017 (legge n. 167/2017), con cui è stato portato a 72 mesi il termine di conservazione dei dati di traffico telefonico e telematico e dei dati relativi alle chiamate senza risposta. Nonostante da più versanti (oltre che da parte dello stesso Garante della Privacy italiano[24]) si fosse fatto notare come tale termine non trovasse alcun corrispettivo nelle legislazioni nazionali degli altri Stati membri – legislazioni che, *per incidens*, si erano attestate su una media di 24 mesi[25] –, la disciplina, derogatoria dell'art. 132 Codice della privacy[26], è andata esente da qualunque censura di legittimità, e conserva tuttora integra la propria efficacia. Il che, *ça va sans dire,* lascia presumere che neppure le severe tempistiche di cui all'art. 10 del d.P.R. 15/2018 andranno incontro ad alcun serio vaglio di compatibilità con il canone di proporzionalità[27] che, lumeggiato altresì dal testo regolamentare in quella che viene pacificamente additata come una delle sue componenti, *id est* quella della "necessità" («I dati

[23] Per ampiezza di rinvii, seppur con specifico riguardo all'identità personale "informatica", cfr. A. MARANDOLA, *La tutela dell'identità personale (informatica), anche del soggetto coinvolto in un processo penale*, in *Processo penale e giustizia* 2017, 3, 371 ss.
[24] Per le relative osservazioni si vada al documento reperibile all'indirizzo *www.garanteprivacy.it.*
[25] Persino la Russia, che certo non svetta tra i Paesi maggiormente "sensibili" alle tutele civili dei propri cittadini, ha fissato il termine di conservazione a (soli) 36 mesi.
[26] Sui contenuti e sulle vicende modificative dell'art. 132 del Codice della privacy vd. *amplius* SIGNORATO, *Contrasto al terrorismo e* data retention: *molte ombre e poche luci*, in *Il nuovo "pacchetto"* antiterrorismo, cit., 78 ss.
[27] Per quel che consta, l'unica pronuncia che ha interessato la disposizione in discussione è stata Cass. civ., Sez. I, 29 agosto 2018, n. 21362, reperibile sul portale *Il penalista*. L'approdo ivi raggiunto dalla Suprema Corte, di sostanziale avallo e soddisfazione per le cautele messe in campo dalla disciplina interna in tema di acquisizione e trattamento dei dati da parte delle forze di polizia, non sembra certo porsi in linea col principio della c.d. "minimizzazione del trattamento" (secondo cui i dati personali devono essere raccolti per finalità determinate, esplicite e lecite nei limiti di quanto necessario per il raggiungimento dello scopo in origine individuato) come ricavabile dal combinato disposto degli artt. 5 e 6 GDPR.

personali oggetto di trattamento sono conservati per un periodo di tempo non superiore a quello *necessario* per il conseguimento delle finalità di polizia di cui all'art. 3 »: art. 10, co. 1) sembra qui ridotto a nulla più che un convitato di pietra[28].

3. ... tipologie di trattamento e "persone sospette"...

La seconda questione problematica che, a tacere del carattere soggettivo di ogni tipo di cernita, si presenta come meritevole di interesse per la molteplicità degli aspetti di garanzia che ne risultano toccati, riguarda la possibilità di un trattamento dei dati personali "differenziato" in ragione della specifica posizione processuale di ciascun soggetto interessato.

Procediamo con ordine.

L'art. 6 della Direttiva 2016/680/UE, rubricato «Distinzione tra diverse categorie di interessati», esorta gli Stati membri affinché «se del caso e nella misura del possibile, operi*no* una chiara distinzione tra i dati personali delle diverse categorie di interessati, quali: a) le persone per le quali vi sono fondati motivi di ritenere che abbiamo commesso o stiano per commettere un reato; b)

[28] Un ambito tematico strettamente correlato a quello analizzato nel corpo del paragrafo, ed altrettanto meritevole di attenzione, sarebbe stato quello dell'impatto della tutela della riservatezza come declinata nella Direttiva, sul c.d. "archivio riservato" contemplato nella più generale riforma della disciplina delle intercettazioni di conversazioni e comunicazioni disegnata dalla legge delega 103/2017. Ma il condizionale e la rinuncia ad una siffatta trattazione si sono imposti in ragione delle sempre più fitte ombre addensatesi sull'operatività del d.lgs. 216/2017, per l'appunto di attuazione della delega. Dopo un primo slittamento decretato con il d.l. 91/2018 (c.d. decreto mille proroghe), l'ultima Legge di Bilancio (145/2018) ne ha rinviato ulteriormente l'entrata in vigore al 1° agosto 2019, palesando così la volontà governativa di prendere tempo, onde por mano all'ennesima rivisitazione della materia. Tutto ciò premesso, vale comunque la pena segnalare come – a fronte dell'istituzione di un luogo virtuale in cui conservare e custodire tutti gli atti afferenti alle operazioni captative quale dovrebbe essere, appunto, l'archivio riservato sotto la direzione e la sorveglianza del pubblico ministero – ci si sia mossi in un'ottica "minimale" dal punto di vista delle garanzie: difatti, se per un verso, all'interno della normativa delegata "sospesa", non risulta *expressis verbis* conferito agli interessati il diritto di rivolgersi all'organo dell'accusa competente per avere conferma della presenza, nella documentazione custodita, di intercettazioni (non acquisite ma) lesive della loro riservatezza, allo scopo di ascoltarne le registrazioni e chiederne la distruzione ai sensi dell'art. 269 comma 2 c.p.p. (cfr. BENE, *La riforma parziale (e il gorilla invisibile)*, in *L'intercettazione di comunicazioni*, a cura di Bene, Bari 2018, 22 ss.), per un altro, nel d.m. 20.4.2018 (*Disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7 commi 1 e 3, D. lgs. 29.12.2017, n. 216)*, di solo un mese antecedente il d.lgs. 51/2018, ci si "accontenta" di imporre l'impiego di «postazioni sicure riservate» per la consultazione degli atti custoditi nell'archivio riservato (vd. per un primo commento SURACI, *D.M. 20 aprile 2018: il c.d. "archivio riservato delle intercettazioni"*, in *Dir. pen. proc.,* 2018, 10, 1258 ss.). Non pare insomma azzardato constatare come, dinanzi all'ennesima "interferenza" della tecnologia negli *itinera* cognitivi del procedimento penale, l'ordinamento italiano non abbia avvertito come "cogente" il dovere di implementare al livello più alto lo *standard* di tutela (pur talora sommessamente) suggerito dalla Direttiva.

le persone condannate per un reato; c) le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato; d) altre parti rispetto a un reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di procedimenti penali conseguenti, le persone che possono fornire informazioni su reati o le persone in contatto o collegate alle persone di cui alle lettere a) e b)». La logica di un tale ammonimento, *expressis verbis* ancorato alla presunzione di innocenza come garantita dalle Carte fondamentali ed avvalorata dai *dicta* dei giudici di Lussemburgo e di Strasburgo (cfr. *Considerando* n. 31 della stessa Direttiva), sarebbe quella di assicurare un più elevato *standard* di tutela per il trattamento dei dati relativi a quei soggetti che non siano destinatari dell'addebito. Del resto, è anche sotto questo profilo – di scarsa adesione, appunto, al principio di innocenza, oltre che all'ennesima declinazione del principio di proporzionalità – che il primo "accostamento" europeo al delicato tema dei trattamenti di dati personali svolti nell'ambito delle attività di indagine penale, la ricordata Decisione Quadro 2008/977/GAI, aveva riportato non poche critiche[29].

In un contesto globale in cui la c.d. *war on terror*, ovvero la lotta al terrorismo internazionale di matrice jihadista, ha progressivamente e costantemente agevolato la trasformazione della sicurezza da interesse pubblico diffuso a diritto fondamentale della persona se non, addirittura, a valore super-primario cui tutti gli altri diritti dovrebbero essere funzionalizzati[30], si è registrata la trasformazione, altrettanto evidente e duratura, dei rapporti esistenti tra processo penale ed attività di raccolta e gestione delle informazioni (c.d. *Intelligence*). Questa tendenza, che taluno ha efficacemente sintetizzato nel lemma «trasmutazione poliziesca»[31] del rito penale, consta altresì di un netto cambio di passo della cultura investigativa che, spinta in questa direzione dalla capacità intrusiva e dalla straordinaria "plasticità" degli strumenti messi a disposizione dall'informatica, è andata vieppiù abbracciando istanze preventive tutte imperniate su un controllo diffuso e generalizzato delle informazioni che possa-

[29] Vd. BORGIA, *Il trattamento di dati personali ai fini di prevenzione, di indagine, di accertamento e di perseguimento di reati o di esecuzione di sanzioni penali: quali passi avanti alla luce dei recenti sviluppi?*, cit., 499 ss.

[30] In questa prospettiva "massimalista" si vedano, ad esempio, MOSCA, *La sicurezza come diritto di libertà. Teoria generale delle politiche di sicurezza*, Padova 2012, 73 ss. e RAIMONDI, *Per l'affermazione della sicurezza pubblica come diritto*, in *Dir. amm.* 2006, 747 ss; *contra* PACE, *Libertà e sicurezza. Cinquant'anni dopo*, in *Dir.soc.* 2013, 177 ss.; e, più di recente, SILVESTRI, *L'individuazione dei diritti della persona*, in *www.penalecontemporaneo.it*, ove si allude alla sicurezza come "interesse fondamentale delle collettività" che al suo interno ingloba singoli diritti fondamentali dei cittadini.

[31] NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *questa Rivista*.

no essere ritenute utili a difendere la sicurezza dello Stato e della collettività da ogni minaccia o aggressione criminale o terroristica[32].

Il *discrimen* tra il comparto della repressione e, quindi, della giurisdizione penale, ed il comparto, invece, della prevenzione, generalmente rimessa ai servizi di informazione per la sicurezza, si è venuto così "opacizzando", o, potremmo dire, "fluidificando"[33].

Non è un caso, per stare ad un esempio di diritto interno, che la già discutibile fattispecie delle intercettazioni *ante delictum* (art. 226 disp. coord. c.p.p.), incentrata, fin dalla sua prima comparsa nella trama codicistica, sull'impalpabile presupposto degli «elementi che giustifichino l'attività di prevenzione»[34], abbia visto man mano estendere il proprio spettro applicativo in occasione di ogni intervento legislativo, per così dire, "emergenziale".

Nei fatti, pur a fronte delle resistenze della dottrina e dei più o meno "ingombranti" silenzi normativi, sia a livello sovranazionale che a livello nazionale vanno aumentando gli aspetti di commistione tra procedimento penale vero e proprio e il complesso delle attività di sicurezza[35]. È, infatti, la giustizia

---

[32] BONINI, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Rivista Aic* 2016, 3, 1 ss.

[33] Fu ORLANDI (*Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis?, in *Riv.it.dir.proc.pen.* 1996, f. 2., 568 ss.) tra i primi a porre in evidenza «l'intima commistione» che si era andata istituendo tra polo repressivo e polo preventivo già subito dopo l'entrata in vigore del Codice Vassalli. E nell'occasione, piuttosto che demonizzare la prassi della c.d. "inchiesta preparatoria", l'Autore invitava non soltanto ad indagare le ragioni di questo fenomeno ma, anche e soprattutto, a regolarne le dinamiche alla stregua di una fase a sé. Più di recente, per ampiezza di riferimenti, cfr. CURTOTTI NAPPI, *Procedimento penale e intelligence in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Processo Penale e Giustizia* 2018, 3, 435 ss.; e KOSTORIS, *Il nuovo "pacchetto" antiterrorismo, tra prevenzione, contrasto in rete e centralizzazione delle indagini*, in *Il nuovo "pacchetto" antiterrorismo,* a cura di Kostoris, Viganò, cit., XV ss.

[34] Cfr. GALLUCCIO MEZIO, sub *art. 226 disp. att.*, in *Codice di procedura penale commentato*, a cura di Giarda, Spangher, Milano 2017, 1061-1069.

[35] «La ragione politico-criminale» – osserva ancora CURTOTTI NAPPI, *Procedimento penale e intelligence in Italia: un'osmosi inevitabile, ancora orfana di regole*, cit., 441 – «trae origine nella criminogenesi di tali fenomeni. La natura "molecolare" delle organizzazioni terroristiche di matrice islamica, priva quasi di un coordinamento centrale ma affidata a singoli individui [...] rende inefficaci i consueti strumenti sia del diritto sostanziale che di quello processuale. Tutto questo » – continua l'Autrice – « ha comportato inevitabilmente un accavallamento tra indagini di tipo penale e indagini di sicurezza, venendo meno o risultando molto affievolita la linea di separazione tra ciò che non è e ciò che già è reato». Ancora, sull'osmosi tra controllo politico e controllo giurisdizionale, sul venir meno dell'impermeabilità tra attività di *intelligence* e attività investigativa che sempre più dovrebbero convergere e coordinarsi, pur nella diversità del ruolo, quanto ad ambienti presi di mira e modalità strategiche per contrastare fenomeni criminali raffinati, tecnicizzati e con alta capacità di movimento cfr. SALVINI, *Da Al Qaeda all'ISIS: la seconda fase del terrorismo islamista. Strumenti giuridici, prime applicazioni e riflessioni culturali*, in *Diritto penale e modernità. Le nuove sfide tra terrorismo, sviluppo tecnologico e garanzie fondamentali,* a cura di Wenin, Fornasari, Trento 2017, 107 ss.

penale nel suo complesso che va vieppiù privilegiando una funzione preventiva *tout court*[36]. Così, è sempre e comunque la logica del (mero) "sospetto" a fondare l'impiego massivo di strumenti anche drasticamente incidenti sui diritti dei loro destinatari che – etichette formali a parte – tradiscono una natura sostanzialmente penale di cui non mutuano, però, il dovuto ossequio ai principi fondamentali[37] o, ancora, a dare una parvenza di giustificazione a certi istituti processuali di caratura ibrida, i quali si collocano, per l'appunto, sull'incerto crinale tra fronte preventivo e fronte repressivo (si pensi alle cc.dd. "indagini proattive" che, di fatto, constano di «tecniche operative miste, anfibie, ambivalenti»[38], finalizzate a prevenire la predisposizione di atti preparatori e la commissione di reati, anche a matrice terroristica[39]).
Peraltro, quasi a voler abbattere ogni residua ipocrisia nei riguardi di questi "arnesi" dalla fisionomia ambigua e dall'ontologico *deficit* di tutele rispetto a quelle assicurate dalle forme investigative *post delictum*, proprio nella Direttiva 2016/680/UE il legislatore europeo ha operato un'omologazione espressa, in punto di disciplina del trattamento, tra le diverse tipologie d'indagine[40]. Il

[36] Più in particolare, sulla «contaminazione teleologica» di un processo penale piegato ad esigenze di difesa sociale e, dunque, a fini di tutela della sicurezza pubblica vd. i preziosi rilievi di MAZZA, *Le persone pericolose (in difesa della presunzione di innocenza)*, in *www.penalecontemporaneo.it.* e, più di recente, quelli di NEGRI, *Diritto costituzionale applicato: destinazione e destino del processo penale*, in *Processo Penale e Giustizia* 2019, 2 (in corso di pubblicazione), il quale, attraverso un'originale lettura delle ordinanze di rimessione alla Corte costituzionale e delle pronunce di quest'ultima, dimostra come il primato della difesa sociale sia di fatto una costante anche all'ombra delle scelte individual-garantistiche della nostra Costituzione.

[37] Il riferimento è chiaramente al sistema delle cc.dd. "misure di prevenzione" che, essendo misure *praeter* o *ante delictum*, sono prive di ancoraggio al fatto di reato e scadono in quelle che vengono comunemente definite come "pene del sospetto" (BRICOLA, *Forme di tutela* ante delictum *e profili costituzionali della prevenzione*, in *Le misure di prevenzione. Atti del Convegno*, Milano 1975, 29 ss.) in ragione del loro alto tasso di afflittività e del vago requisito della pericolosità che ne forma il sostrato. La letteratura, sul punto, è sterminata: ci si limita a citare PADOVANI, *Misure di sicurezza e misure di prevenzione*, Pisa 2014, 196 ss. e ORLANDI, *Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali*, in *La giustizia penale preventiva*, Milano 2016, 5 ss.

[38] Vd. ancora, incisivamente, NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, *ibidem*.

[39] Vd. *Risoluzione del XVIII Congresso internazionale di diritto penale*, Istanbul, 20-27 settembre 2009, in *Riv. it. proc.* 2010, 333 ss; SIGNORATO, *Il trattamento dei dati personali per le finalità di polizia: la nuova disciplina prevista dall'art. 53 Codice Privacy e gli scenari europei*, cit., 99; LA PISCOPIA, *Rilevanza penale del cosiddetto* Habeas Data *in materia di terrorismo internazionale*, in *Periodico di Diritto e Procedura penale militare* 2017, n.3, 5 ss.; e, *last but not least*, SPATARO, *Politiche della sicurezza e diritti fondamentali*, in *Terrorismo internazionale, politiche della sicurezza, diritti fondamentali*, in *Gli Speciali Questione Giustizia*, 2016, 188 ss., il quale offre un'ampia panoramica delle attività attraverso le quali gli organi a vario titolo competenti nel sistema legislativo italiano procedono all'analisi di dati con finalità investigative.

[40] Ritiene che la sfida così cristallizzata nella Direttiva sia stata lanciata dal legislatore dell'Unione «quasi inconsapevolmente», come se quest'ultimo, in fondo, si fosse limitato a "fotografare" quella che era la

che – si è altresì auspicato[41] – avrebbe potuto comportare un «innalzamento» dello *standard* tutorio imposto anche al titolare del trattamento a fini preventivi. Eppure – ed è ciò che sembra emergere con particolare nitore dalla prospettiva offerta dall'art. 6 di cui qui si discute – non è sufficiente prevedere, a valle, un livellamento dei diritti e delle facoltà riconosciute a ciascun interessato, quale che sia la "qualifica" di quest'ultimo, per illudersi di aver colmato, a monte, il *gap* di garanzie che presiede all'attribuzione della qualifica di "sospettato" funzionale, tra l'altro, alla diversificazione del regime trattamentale.
Nel testo europeo – si badi bene – nemmeno si è tentato di specificare i presupposti in forza dei quali si possono ritenere legittimamente integrati i "fondati motivi" per temere che taluno "stia per commettere un reato"; e nulla si è detto in merito all'autorità competente a conferire (anche) formalmente un siffatto *status* soggettivo da cui poi far discendere, tra i molteplici altri effetti, un trattamento meno "impattante" sull'*habeas data* del singolo.
Si tratta, a ben vedere, di un silenzio fin troppo loquace. Ché, nella migliore delle ipotesi, l'omissione denuncia la malcelata consapevolezza, da parte del legislatore dell'Unione, di non poter affrontare qui ed ora un tema tanto complesso e, al contempo, tanto bisognoso di "rifondazione" come quello per l'appunto rappresentato dalla categoria dei soggetti "pericolosi" alle prese e con le dinamiche dell'accertamento giurisdizionale e, soprattutto, con tutte quelle attività condotte dalle più svariate autorità amministrative in difetto di un'ascrizione di responsabilità ancora lungi dal delinearsi[42].
Ad essere in gioco, difatti, non è un problema meramente definitorio, ma l'opportunità stessa di ridurre le fughe dalla "legalità" e le distorsioni ineluttabilmente veicolate da approcci unilaterali a tematiche che, invece, reclamano una razionalità di stampo olistico.
Ancora: ammesso e non concesso che un'indicazione così "slabbrata" di sog-

realtà dei fatti a tutti gli effetti, CURTOTTI NAPPI, *Procedimento penale e intelligence in Italia: un'osmosi inevitabile, ancora orfana di regole*, cit., 445.

[41] SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., 92.

[42] Sulle innumerevoli aporie sottese al tema di una "pericolosità" riconnessa all'imputazione *tout court*, che come tale prescinde dalla valutazione di condotte specifiche tenute dall'indagato/imputato nel corso del processo, si veda ancora MAZZA, *Le persone pericolose (in difesa della presunzione d'innocenza)*, cit., 2 ss. Più diffusamente, sull'inattingibilità strutturale del giudizio prognostico di pericolosità, sulla sua sostanziale non verificabilità e falsificabilità sul piano scientifico, e sul suo atteggiarsi, ad ogni buon conto, a canone fondante di istituti basati su presupposti profondamente diversi ed orientati a finalità eterogenee cfr., tra gli altri, MARTINI, *Essere pericolosi. Giudizi soggettivi e misure personali*, Torino 2017, 1 ss. «La pericolosità» osserva l'Autore (7) – si mostra [...] come un dato ipostatizzato, del quale il sistema giuridico subisce l'impatto, la sublimazione di una quantità imprecisata di percezioni individuali, che si esprimono in previsioni, convinzioni precognite, di quello che sarà il comportamento futuro di chi ha dato una determinata prova di sé, nel passato»

getto sospettato come quella giustappunto fornita dalla lettera dell'art. 6 della Direttiva, non si ponga in rotta di collisione con i fondamenti di qualsiasi sistema processualpenalistico che si voglia definire liberale, occorre interrogarsi circa la presenza, all'interno dell'apparato normativo eurounitario, di eventuali altri rinvii alla categoria di "persona sospetta", magari (più) denotativi in punto di determinatezza, cui l'interprete possa utilmente raccordarsi.

Orbene, essendo tra quelle di più recente introduzione, a balzare subito agli occhi è la fattispecie soggettiva di "sospettato" delineata dalla Direttiva 2016/681/UE. Quest'ultima, approvata dal Parlamento europeo e dal Consiglio nell'ambito del più ampio ventaglio di provvedimenti sulla *data protection* di cui si è detto, si occupa di un settore specifico, ossia dell'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi[43].

Premesso che per dati PNR (*Passenger Name Record*) s'intendono le informazioni fornite dai passeggeri e raccolte dalle compagnie aeree durante la prenotazione dei voli e le procedure di *check-in* (quali data di viaggio, itinerario, indirizzo ed estremi dei passeggeri, informazioni sul bagaglio e sulle modalità di pagamento: vd. Allegato I della Direttiva)[44], l'obiettivo dichiarato del legislatore europeo era quello di rafforzare il sistema di controllo relativamente a tutti i passeggeri di voli extra-UE[45]. In quest'ottica, ad intervenire nella "catena di trattamento" sono, oltre alle autorità pubbliche competenti, il vettore aereo di volta in volta chiamato in causa e la c.d. "unità di informazione sui passeggeri" (UIP), designata da ciascun Stato membro ai sensi dell'art. 4. Sarà quindi tale Unità, sulla scorta di criteri che dovrebbero ispirarsi ai principi di necessità e di proporzionalità, ad effettuare le analisi di trattamento finalizzate alle specifiche esigenze di prevenzione e repressione di fatti di terrorismo o di altri "reati gravi".

È nondimeno sufficiente l'avvertimento iscritto nel *Considerando n.* 7 della Direttiva stessa[46] a mettere in guardia tanto dalla pervasività di questo mecca-

[43] Di cui dà dettagliato elenco l'allegato II della Direttiva 2016/681.

[44] È dunque solo un'illusione, a ben vedere, la convinzione che la Direttiva 681 goda di un ambito di raccolta più ristretto rispetto a quello potenzialmente indefinito della Direttiva 680: come si ricava già dall'esemplificazione riprodotta nel testo, i dati contenuti dal PNR sono numerosissimi e tutti inscindibilmente legati all'individuo.

[45] Si definisce "volo extra-UE" un volo di linea o non di linea effettuato da un vettore aereo in provenienza da un Paese terzo e che deve atterrare nel territorio di uno Stato membro oppure in partenza dal territorio di uno Stato membro e che deve atterrare in un Paese terzo. Nulla esclude – stando a quanto previsto dall'art. 2 – che i singoli Stati membri, previa adeguata comunicazione alla Commissione UE, estendano la Direttiva *de qua* anche ai voli intra-UE: è stata questa, ad esempio, l'opzione dell'Italia (cfr. art. 1 comma 1, lett. *a)* del d.lgs. 21 maggio 2018, n. 53 di attuazione della Direttiva).

[46] «La valutazione dei dati PNR consente l'identificazione di persone mai sospettate di reati di terrorismo

nismo di controllo[47], quanto dal suo elevato tasso di errore[48]. Ed una "confessione" siffatta, relativa appunto a quello che potrebbe definirsi un vero e proprio *bug* del sistema di *listing*, non può di certo tranquillizzare. Del resto, l'assunto di partenza, fin qui non ancora declinato nella sua carica più dirompente, è che tutti i comuni cittadini che prendono un volo proveniente o diretto verso un Paese terzo siano, solo e soltanto in quanto tali, "potenziali sospetti"[49]. Poi, una volta "processati" i loro PNR *code* secondo criteri auspicabilmente affidabili[50] e periodicamente aggiornati[51] (... criteri che – e qui si noti il paradosso – quale che sia la loro insondabile cifra di "rigore", si trovano però ad operare su dati *ab origine* non verificati, in quanto rilasciati dal passeggero quando acquista il biglietto o effettua il *check-in*[52]), a fronte di un eventuale *match* positivo, quegli stessi individui potranno divenire "sospettati" a pieno titolo.

---

o di reati gravi prima di tale valutazione per cui è opportuno che le autorità competenti procedano a ulteriori verifiche»; «i criteri di valutazione dovrebbero essere definiti in maniera da ridurre al minimo il numero di persone innocenti erroneamente identificate dal sistema».

[47] ...definibile come vero e proprio "controllo di massa" in quanto non diretto a specifiche categorie di soggetti.

[48] Si vedano a questo proposito le osservazioni critiche contenute nei pareri rilasciati dal Garante europeo della protezione dei dati in merito alle diverse proposte di Direttiva succedutesi nel tempo: cfr., tra gli altri, i testi pubblicati in GUUE 2011/C 181/02 e 2010/C 357.

[49] In termini simili si esprimeva l'Avvocato Generale Paolo Mengozzi nelle Conclusioni presentate l'8 settembre 2016 in relazione alla domanda di parere avanzata dal Parlamento Europeo (Parere 1/15) sul Progetto di accordo tra il Canada e l'Unione europea sul trasferimento e il trattamento di dati del codice di prenotazione (*www.curia.europa.eu*). «L'ingerenza determinata dall'accordo previsto ha una portata certa e una gravità non trascurabile. Infatti, da un lato, essa riguarda, in modo sistematico, tutti i passeggeri che usufruiscono dei collegamenti aerei tra il Canada e l'Unione europea, vale a dire varie decine di milioni di persone all'anno. D'altro lato, [...] , non si può ignorare il fatto che il trasferimento di quantitativi ingenti di dati personali dei passeggeri aerei, in cui sono compresi dati delicati, che necessitano, per definizione, di un trattamento automatizzato, nonché la conservazione di tali dati per un periodo di cinque anni mirano a consentire un confronto, eventualmente retrospettivo, di tali dati con modelli comportamentali predefiniti "a rischio" o "preoccupanti", collegati ad attività terroristiche e/o di criminalità transnazionale grave, al fine di identificare persone fino a quel momento sconosciute ai servizi di polizia o non sospette. Orbene, tali caratteristiche, apparentemente inerenti al regime PNR istituito dall'accordo previsto, possono far sorgere la spiacevole sensazione che tutti i viaggiatori interessati siano trasformati in potenziali sospetti» (§ 176).

[50] L'impiego dell'avverbio ottativo si giustifica in ragione dell'opzione "debole" sottesa alla Direttiva, ovvero in ragione della scelta di non definire i contenuti dei suddetti criteri a livello centrale, lasciandone piuttosto l'elaborazione alle singole Unità nazionali.

[51] Vd. in questo senso i moniti lanciati dai giudici di Lussemburgo nella pronuncia circa la (non) compatibilità della disciplina fissata dall'Accordo PNR UE-Canada con i Trattati UE (*www.curia.europa.eu*) e, per un commento denso di spunti di riflessione, VEDASCHI, *L'accordo internazionale sui dati dei passeggeri aviotrasportati (ONR) alla luce delle indicazioni della Corte di Giustizia dell'Unione Europea*, in *Giur. cot.,* 2017, 1913 ss.

[52] Così, opportunamente, BONFANTI, Big data e *polizia predittiva: riflessioni in tema di protezione del diritto alla* privacy *e dei dati personali*, in *MediaLaws-Rivista dir. Media* 2018, 3, 11.

Non si può dunque non cogliere tutta l'opacità e l'evanescenza di una categoria soggettiva così (poco) strutturata, opacità ed evanescenza che non trovano rimedi compensativi né in una "procedimentalizzazione" solo apparentemente tassativizzata, né, come si è visto, nelle indicazioni disseminate in altri testi normativi e facenti riferimento al medesimo presupposto operativo dell'"essere sospettato".

Pertanto – e si ritorna al *focus* della questione qui originariamente prospettata – non stupisce che lo stesso legislatore italiano, chiamato ad implementare la Direttiva 2016/680/UE, abbia scelto la soluzione più comoda ed immediata, ossia quella di non "trasporre" in nessuna delle fattispecie soggettive nostrane la categoria delle «persone per le quali vi sono fondati motivi di ritenere che [...] stiano per commettere un reato»[53]. Col risultato, scontato, di accrescere i "vuoti di tutela" ed il livello di arbitrio rimesso alle forze di polizia le quali – esemplificando ancora – al cospetto di un trattamento-dati riferibile a colui che sia attinto da una misura precauzionale giustificata da meri indici sintomatici, rivelatori di pericolosità sociale, sono di fatto legittimate ad eludere ogni distinguo rispetto al trattamento-dati di coloro che risultino già destinatari di un addebito formalizzato di un fatto di reato.

Con buona pace, appunto, del principio di non colpevolezza *in apicibus* evocato.

La non rinviabilità, insomma, di un'operazione di razionalizzazione delle diverse discipline appena richiamate non sembrerebbe abbisognare di ulteriori argomenti. Purtroppo, nonostante la perenne attualità della massima ciceroniana secondo cui *silent enim leges inter arma*, l'Unione europea non cessa di tradire, sotto molteplici versanti, una concezione (prevalentemente) "efficientistica" del processo penale, inteso alla stregua di una «barriera da ergere a fronte della minaccia rappresentata da gravi forme di criminalità organizzata e transnazionale, compreso il terrorismo»[54]. Non è un caso, del resto, che proprio con le parole or ora richiamate si alludesse alla proposta di direttiva in tema di presunzione d'innocenza, proposta che, qualche anno più tardi, sarebbe poi stata licenziata dal Parlamento europeo e dal Consiglio nella sua

[53] Il d.lgs. 51 del 2018 ha trasposto la categorizzazione *de quo agitur* nella lettera dell'art. 4 comma 1, secondo cui gli interessati dovranno essere distinti in persone sottoposte ad indagine; imputati; persone sottoposte ad indagine o imputate in un procedimento connesso o collegato; persone condannate con sentenza definitiva; persone offese dal reato e, infine, parti civili. Balza subito agli occhi come, in un'immaginaria tavola di comparazione, difetti nel testo domestico l'enucleazione di un gruppo di soggetti "trattandi" a cui ricondurre quelli che il legislatore comunitario ha pure vagamente individuato come "coloro a carico dei quali vi siano fondati motivi di ritenere che stiano per commettere un reato".

[54] MAZZA, *Una deludente proposta in tema di presunzione d'innocenza*, in *questa Rivista*.

versione definitiva (Direttiva 2016/343/UE)[55].

4. ... decisione giudiziale penale e ruolo della "macchina".

Ed è proprio allo scopo di verificare il grado di radicamento di una visione così eludente e deludente come quella finora riscontrata nei confronti di uno dei metavalori su cui avrebbe dovuto fondarsi il "giusto processo penale europeo", che l'ultimo dei capitoli tematici che ci proponiamo di esaminare nel quadro normativo del trattamento dei dati personali per finalità di *law enforcement*, è rappresentato dal regime concernente i processi decisionali automatizzati.

Innanzitutto: dal punto di vista prettamente testuale, mutuando le disposizioni del GDPR[56], la Direttiva 2016/680/UE (art. 11), sembra consacrare il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati, tra cui la profilazione[57].

Preso atto del ruolo sempre più decisivo assunto dall'informatica e dalla digitalizzazione nell'ambito del diritto e, più in particolare, della reingegnerizzazione di tutti i processi che da tali applicazioni possono discendere, il legislatore europeo ha voluto dimostrare, (anche) in termini di diritto positivo, di non ignorare i rischi che, per le libertà ed i diritti dell'interessato, possono derivare dall'impiego di algoritmi complessi[58], dallo sviluppo dei *Big Data* e

---

[55] Cfr. le severe censure dell'Unione delle Camere Penali Italiane-Osservatorio Europa: *La Direttiva (UE) 2016/343 sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali: più ombre che luci*, in *www.camerepenali.it*.

[56] ... e in particolare quelle dell'art. 22 che, a sua volta, riprende e rinnova quanto contenuto nell'art. 15 della Direttiva 1995/46: cfr. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., 34 ss.

[57] Finora prevalentemente adottata nel campo delle attività commerciali, la profilazione consta di «una tecnica di trattamento automatico, mediante algoritmi, di dati relativi a quantità numericamente anche molto elevate di persone, per attribuire a ciascuna di esse un profilo, cioè una categoria predefinita e delineata attraverso parametri che il responsabile del trattamento considera necessari alla sua ricerca, al raggiungimento del suo scopo»: vd. DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Dir. informatica* 2013, 587. Il legislatore europeo, dal canto suo, ne offre la seguente definizione tecnica: «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» (art. 3 n. 4 della Direttiva 2016/680). Con specifica attenzione, poi, al *criminal profiling* e alle nebulosità che ne contraddistinguono tecniche ed epiloghi, si rinvia al prezioso contributo di LUPARIA, *Il* profiling *dell'autore di reato*, in *Le indagini atipiche*, a cura di Scalfati, Torino 2014, 329 ss. e alla bibliografia ivi richiamata.

[58] «Algorithms need not be software: in the broadest sense, they are encoded procedures for transforming input data into a desired output, based on specified calculations. The procedures name both a problem and the steps by which it should be solved. Instructions for navigation may be considered an algorithm, or the mathematical formulas required to predict the movement of a celestial body across the sky» (T. GILLESPIE, *The relevance of Algorithms*, 2014) citato dallo studio del Consiglio di Europa dal

dalla crescita esponenziale della potenza di calcolo, ossia, per dirla con espressione sintetica, dalla c.d. "giustizia predittiva".
Un sintagma, quest'ultimo, dai contenuti abbastanza ampi ed ambigui, giacché suscettibile di ricomprendere «un ventaglio di opzioni che hanno in comune l'applicazione di sofisticate tecnologie sia con finalità di carattere analitico/induttivo (si scoprono *pattern* decisionali o *pattern* comportamentali analizzando e processando dati che riguardano casi e decisioni già avvenuti) sia con finalità prospettico-predittivo (si individuano propensioni e su questa base vengono valutate le probabilità con le quali si può prevedere che la decisione del giudice [...] converga su un punto che possiamo definire focale)»[59].
È fatto notorio, invero, come da decenni ormai, in taluni ordinamenti, come quello statunitense, vengano utilizzati "sistemi esperti" per misurare il rischio di recidiva e, dunque, per concedere o meno la libertà sotto cauzione in sede investigativa, o determinare l'entità della pena[60] o della misura alternativa alla detenzione, in fase di deliberazione. Per non dire, ancora, delle tecniche di riconoscimento facciale già ben sviluppate in Paesi come la Cina o, ancora, del sistema *smart* denominato *IBorderCtrl* che, finanziato nell'ambito di Horizon 2020 dalla Commissione Europea e sperimentato a breve in Ungheria, Lettonia e Grecia, avrà il compito di rilevare, anche attraverso l'analisi di comportamenti non verbali, le presunte menzogne di coloro che stanno per attraversare le frontiere UE e, dunque, di individuare eventuali migranti illegali latori di minacce terroristiche[61].

---

titolo *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications)*, DGI (2017)12.

[59] Vd. efficacemente CASTELLI, PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi*, in *Quest.Giust.* 15 maggio 2018, § 1. Sulla difficoltà di rinvenire un *discrimen* netto tra *software* a carattere valutativo e *software* a carattere meramente descrittivo cfr. SIGNORATO, *Le indagini digitali*, cit., 100.

[60] Si cita sempre, in proposito, il caso Loomis: nel febbraio 2013 un cittadino statunitense, Eric Loomis, veniva arrestato per due reati che potremmo qualificare come ricettazione di un'auto e resistenza a pubblico ufficiale. Per tali fatti Loomis veniva condannato alla pena di sei anni di reclusione, una pena particolarmente severa determinata sulla scorta dell'alto punteggio (*score*) risultante a suo carico da COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), un algoritmo predittivo di valutazione del rischio di recidiva. Cfr. *State v. Loomis, Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing*, reperibile all'indirizzo *www.harvardlawreview.org*.

[61] Sui dettagli del progetto europeo vd. *www.cordis.europa.eu* e sulle modalità operative del c.d. "poliziotto virtuale" vd. *www.iborderctrl.eu.* Per un quadro più completo delle tecniche di utilizzo di *big data* da parte delle forze dell'ordine nello svolgimento delle funzioni di protezione della sicurezza pubblica e di prevenzione del crimine vd., ancora, BONFANTI, Big data e *polizia predittiva: riflessioni in tema di protezione del diritto alla* privacy *e dei dati personali*, cit., 2 ss. Premesso che tra le fonti di "approvvigionamento" di informazioni vi sono, non soltanto le banche dati elaborate dalle stesse forze dell'ordine ma, altresì, quelle acquisite dai *databrokers*, e quelle estrapolate dai *social networks* e dagli impianti a circuito chiuso, gli "incroci" algoritmicamente operati sono funzionali alla previsione della

Ora, lasciando da parte il peculiare angolo prospettico della prevenzione (che pure non può dirsi del tutto slegata dalla fase dell'accertamento sulle cui "porosità" sono già stati forniti molti *caveat*...), dovrebbero essere sufficienti questi pochi *flash* per far emergere le possibili tensioni che un impiego poco meditato di questi "sistemi esperti" può rovesciare sul versante delle garanzie fondamentali del processo penale.

Ferma infatti l'indubbia appetibilità – in un'epoca caratterizzata da un'"esplosione" del sistema delle fonti e dalla difficoltà del legislatore di ricondurre il caos normativo a razionalità[62] – di una prevedibilità delle decisioni giudiziarie come quella per l'appunto apparentemente promessa dalle enormi potenzialità computazionali della tecnologia digitale, di una prevedibilità, cioè, che parrebbe addirittura rimandare ad un ideale di "calcolabilità del diritto" di irtiana se non weberiana memoria, non possono certo essere ignorati gli *essentialia* della decisione e della discrezionalità giudiziale penale.

Al netto, infatti, del tasso di affidabilità di questi sistemi, ancora tutto da verificare in seno alle diverse comunità scientifiche di riferimento[63], sembra paci-

---

commissione di reati e della loro localizzazione (*crime hotspot*) da un lato, e all'elaborazione di profili individuali (*predictive composite*) dall'altro.

Con specifico riguardo alla prima delle finalità richiamate, può addursi un esempio domestico che ha guadagnato di recente gli onori della cronaca (DELLA SALA, *"*XLaw*": un algoritmo può davvero prevedere (e impedire) un reato?*, in *Il Fatto quotidiano*, e IASELLI, *X-Law:la polizia predittiva è realtà*, reperibile all'indirizzo *www.altalex.com*: trattasi del software chiamato "XLaw", per l'appunto basato su un algoritmo che è in grado di identificare luoghi, orari e condizioni che rendono più probabile la commissione di un reato; sulla scorta di questi scenari probabilistici, vengono dunque inviate le volanti della polizia con il risultato che, laddove dovesse davvero verificarsi un crimine, esse si troverebbero già nei paraggi e sarebbe così ottimizzato l'uso delle risorse.

[62] Sottolinea come, essendo la prevedibilità della decisione giudiziale «un valore» per così dire sistemico, tutti gli attori istituzionali dell'ordinamento dovrebbero farsi carico della sua difesa e della sua promozione VIGANÒ, *Il principio di prevedibilità della decisione giudiziale in materia penale*, in *www.penalecontemporaneo.it*. Ancora: è proprio al tentativo di ridurre i sempre più frequenti contrasti giurisprudenziali in ordine al medesimo profilo giuridico che deve ascriversi l'attribuzione di valore per così dire "paranormativo" alle pronunce del giudice di legittimità nel suo più alto consesso. Sulla riscrittura dell'art. 618 c.p.p. ad opera della c.d. "riforma Orlando" vd., con pluralità di accenti, DE CARO, *Il ricorso per Cassazione*, in *La riforma della giustizia penale*, *Commento alla legge 23 giugno 2017, n. 103*, a cura di A. Scalfati, Torino 2017, 245-248; FIDELBO, *Verso il sistema del precedente? Sezioni Unite e principio di diritto*, in *La riforma delle impugnazioni tra carenze sistematiche e incertezze applicative, (Commento alla legge 23 giugno 2017, n. 103 e al d.lgs. 6 febbraio 2018, n. 11)*, Torino 2018, 115 ss.; MAZZA, *Le garanzie deboli nel relativismo della Corte di Strasburgo,* in *Criminalia* 2017, 464 ss. e MONACO, *Riforma Orlando: come cambia il giudizio in Cassazione*, in *La riforma Orlando. Modifiche al Codice penale, Codice di procedura penale e Ordinamento penitenziario*, a cura di Spangher, Pisa 2017, 291-292.

[63] Basterebbe pensare, in proposito, alle contestazioni mosse dallo stesso Loomis nei confronti dell'algoritmo COMPAS, il cui meccanismo di funzionamento, in quanto non pubblicamente noto, non era nemmeno accertabile sotto il profilo della validità scientifica. Difatti, onde comprendere come opera un software, occorre avere l'accesso al suo codice sorgente e, così, poterlo leggere. Si definisce

fica l'irriducibilità ad un mero modello matematico dello *jus dicere* penale e, conseguentemente, l'impossibilità di sostituire il giudice-persona fisica col c.d. "giudice-robot".

Sebbene non manchino teorizzazioni circa la possibilità che un algoritmo possa in piena autonomia "macinare" una sentenza, di certo un tale scenario non può trovare legittimazione nel settore della giustizia penale: diversamente, infatti, da certune controversie civili o amministrative che potremmo definire "seriali" o, comunque, "routinarie", in cui le attività connesse alla *res iudicanda* sono per lo più a discrezionalità vincolata[64], il giudizio penale presenta problemi di accertamento e orizzonti valutativi che, pur sulla base di fondamentali principi garantistici, necessitano, di volta in volta, di uno scavo ermeneutico e ricostruttivo suscettibile di essere congruamente operato soltanto dal giudice "in persona"[65]. Quand'anche, corrispondentemente al progressivo ampliarsi delle basi documentali di riferimento, venga ad elevarsi lo *standard* qualitativo, di precisione e di accuratezza, dei risultati prodotti dai cc.dd. "sistemi esperti"[66], il calcolo algoritmico non potrà comunque mai svolgere il ruolo di "dittatore"[67] ma dovrà, semmai, fungere da indicatore strumentale per orientare il libero convincimento del giudice. Un convincimento che, lungi dal potersi adagiare sui comodi declivi dell'arbitrio, non può neppure irrigidirsi, tuttavia, in una sorta di "matematizzazione" dei criteri ermeneutici o,

---

per contro "proprietario" un programma di cui non sia possibile conoscere il codice-base e, conseguentemente, il funzionamento e le scelte "a monte" dei suoi programmatori (cfr. *amplius* L. LESSIG, *Cultura libera*, Milano 2007, *passim*). Ancora, in merito alla necessaria verificabilità dei processi di analisi che possono determinare la formazione di decisioni "gravose" a carico dell'indagato, cfr. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, cit., 6. Di sicuro nemmeno gli algoritmi sono neutrali: essi, infatti, possono essere latori di "pregiudizi" di calcolo che, applicati su larga scala, possono dare luogo a vere e proprie storture e discriminazioni. Vd. ancora, *infra*, nel testo di questo paragrafo.

[64] Cfr. VIOLA, *Interpretazione della legge con modelli matematici*, Milano 2017, *passim* il quale prospetta come via perseguibile la costruzione di algoritmi su base logica facendo leva sull'art. 12 disp.prel.

[65] ... e, a maggior ragione, in un contesto in continua trasformazione come quello attuale, in cui – anche per l'influenza degli ordinamenti sovranazionali e delle pronunzie delle Corti europee – il giudice è di fatto chiamato ad «un approccio duttile, condotto nella logica del bilanciamento» e «sempre più ispirato a razionalità pratica»: cfr. KOSTORIS, *Processo penale e paradigmi europei*, cit., 233 ss.

[66] Lo dimostra, in via del tutto empirica, il progressivo e costante affinamento degli esiti delle traduzioni affidate a piattaforme come Google traduttore. Evidentemente, il sempre maggior numero di dati (nel caso di specie, espressioni e vocaboli) inseriti nella "macchina", consentono a quest'ultima di rendere traduzioni vieppiù corrette e verosimili.

[67] ...mutuando così il titolo, felice, del libro di ZELLINI, *La dittatura del calcolo* Milano 2018, che, a sua volta, ricorda «la dittatura dell'algoritmo» di rodotiana ascendenza: cfr. RODOTÀ, *Il diritto di avere diritti*, Bari 2012, 398. Più di recente, hanno parlato di una vera e propria «*hubris* numérique» GARAPON, LASSÈGUE, *Justice digitale. Révolution graphique et rupture anthropologique*, Paris 2018, 328.

comunque, ridursi ad una serie di pericolosi automatismi decisionali[68].
Alla luce di queste considerazioni, la scelta – del legislatore europeo prima, e di quello italiano poi[69] – di sancire il divieto di decisioni penali che, incidendo negativamente sulla sfera soggettiva dell'individuo, non contemplino alcun intervento umano, sembrerebbe del tutto in linea, tra l'altro, col nostro modello legale di motivazione della sentenza in virtù del quale, ad esempio, la valutazione della pericolosità del soggetto non può di certo esaurirsi nella mera presa d'atto dei suoi precedenti (verifica questa che, essendo puramente quantitativa, sarebbe ovviamente ben assolvibile da un programma informatico all'uopo deputato...).
Proprio perché «il dato su cui si deve esprimere il giudizio attinge contemporaneamente la sfera conoscitiva ed emozionale» e «non esiste una sfera conoscitiva separata da una sfera emozionale»[70]; proprio perché la componente empatica ed emozionale del giudizio risulta per un verso (quantomeno allo stato) inimitabile ad opera dei sistemi di intelligenza artificiale e, per l'altro, irrinunciabile da parte di un processo penale che trova (anche) in essa il suo contrassegno assiologico (come ci dimostra, tra le altre, una disposizione del codice di rito quale l'art. 525 c.p.p. che, per l'appunto, dichiara la centralità della dimensione emotiva nella logica del giudizio, imponendo il contatto diretto tra il "giudice uomo" ed il "materiale umano" che egli andrà a sindaca-

[68] Del resto, ancora di recente e con la consueta efficacia, FERRUA (voce *Regole di giudizio (diritto processuale penale)*, in *Enc. dir., Annali*, X, Milano 2017, 748) ci ricorda come la metodologia sottesa al procedimento di valutazione (legale e razionale) delle prove sia «troppo complessa e sfumata» per essere rimessa ad altri che al giudice. Soltanto il giudice – e non il legislatore, né un sistema cibernetico (pur) avanzato – può determinare il valore assunto da prove legittimamente acquisite. Sulla stessa linea di ragionamento che guarda all'«azione del giudicare» come ad «un'azione eminentemente complessa la quale assorbe, fonde e compendia le mozioni più svariate, non solo di tecnica giuridica, ma istanze affettive, sociali e culturali» e che, in quanto tale, non può certamente essere ridotta «ad una gestione asettica della vicenda processuale, fondata su obsolete gerarchie di "prove tariffate"» LANZA, *Emozioni e libero convincimento nella decisione del giudice penale*, in *Criminalia* 2011, 365 ss.

[69] Cfr. art. 8 d.lgs. 51/2018 rubricato «Processo decisionale automatizzato relativo alle persone fisiche», i cui contenuti – ed in particolare il comma 1 («Sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato ...») – ricalcano pedissequamente quelli della disposizione unitaria.

[70] DINACCI, voce *Regole di giudizio (Dir.proc.pen.)*, in *Dig. Pen.* Torino 2014, VIII agg., 644 ss. Sulla multifattorialità dell'operazione decisoria la letteratura è assai ampia: si vedano, per tutti, il contributo – ormai un vero e proprio classico – di AMODIO, voce *Motivazione della sentenza penale*, in *Enciclopedia del Diritto*, XXVII, Milano 1977, 181 ss; di FORZA, *Razionalità ed emozioni nel giudicare*, in *Criminalia* 2011, 353 ss.; e, da ultimo, di LORUSSO, *Il diritto alla motivazione*, in *www.penalecontemporaeo.it*. In tutti e tre i lavori, nondimeno, l'accento viene posto più sul "disagio" derivante dalla difficoltà di individuare ed "incasellare" le componenti intuitive che concorrono alla formulazione dell'enunciato finale, che sul valore aggiunto che esse, una volta debitamente governate, tributano alla funzione giurisdizionale.

re), non ci si può rassegnare ad una decisione esclusivamente "robotica".
Messi diligentemente da parte i casi di "emotività deviata e deviante" rispetto ai quali l'ordinamento offre strumenti rimediali come l'astensione e la ricusazione; accuratamente disvelate le insidie cognitive e i *biases* in cui il giudice persona può cadere laddove li ignori[71], deve ritenersi meritevole di sicuro apprezzamento una linea di politica normativa che – almeno in via di principio – sembra salvaguardare l'"umanità" della giurisdizione intesa come combinato disposto di emozione e ragione, rinvigorendo la garanzia di un giudice che sia capace "cogliere" la concretezza di ciascun caso sottoposto alla sua attenzione, risultando così (e soltanto così) pienamente razionale[72]. Si è precisato, volutamente, "almeno in via di principio": difatti, deve preoccupare, e non poco, la sostanziale "frangibilità" di un divieto come quello formulato dalla Direttiva, poi ripreso dall'art. 8 d.lgs. 51/2018, che si accontenta di corredare della garanzia della riserva di legge («salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge»[73]) la previsione di eventuali deroghe e, dunque, l'ammissibilità di modelli decisionali automatizzati.
Tra l'estremo di un'ammirazione entusiastica e quello, per contro, di un distacco timoroso nei riguardi dell'accesso al proscenio dell'accertamento penale da parte dei progressi della robotica, dell'informatica e delle conquiste nel campo dell'intelligenza artificiale[74], una "laica" via di mezzo pare appunto rin-

[71] Se ne vedano alcune esemplificazioni (tra cui l'effetto ancoraggio, la fallacia della congiunzione, la *tunnel vision*) in CEVOLANI, CRUPI, *Come ragionano i giudici: razionalità, euristiche e illusioni cognitive*, in *Criminalia* 2017, 181 ss. e, da ultimo, in FORZA, MENEGON, RUMIATI, *Il giudice emotivo*, Bologna 2017, 146-152. In quest'ultimo testo, anche sulla scorta dei contributi più recenti in materia di psicologia empirica e di neuroscienze, il ruolo delle emozioni "buone" nel processo decisionale è ampiamente valorizzato, giacché – come si legge nella *Postfazione* di IACOVIELLO (220) – «il fatto ha più dimensioni, più strati: la ragione riesce a sondare gli strati superficiali, ma è l'emozione che penetra negli strati profondi attraverso l'intuito. È l'emozione un propellente efficace per la ricerca di ipotesi e di prove».

[72] Parla di una «compassione appropriata» e, ancora, di «emozioni» che sono «potenziali alleate, se non elementi costitutivi, della discussione razionale» NUSSABUM, *L'intelligenza delle emozioni*, Bologna 2004, 532 e 540.

[73] ... «cui competerà predisporre adeguate garanzie per i diritti e le libertà dell'interessato e, in ogni caso, assicurargli il diritto a ottenere l'intervento umano (non è chiaro se a integrazione, sostituzione e correzione dell'algoritmo»: cfr., con toni non meno scettici dei nostri, L. PULITO, *Il trattamento dei dati personali in ambito penale e l'uso del* passenger name record *per contrastare il terrorismo e altri gravi reati*, cit., 1148. A questo proposito l'unico tentativo di puntualizzazione lo si rintraccia al *Considerando* n. 38 della stessa Direttiva, a detta del quale il diritto all'intervento umano dovrebbe tradursi nel diritto di «esprimere la propria opinione, di ottenere una spiegazione della decisione raggiunta [...] e di impugnare la decisione» da parte dell'interessato.

[74] Da ultimo, offre una descrizione suggestiva dell'atteggiamento *naturaliter* "passatista" dell'intelligenza umana dinanzi a qualunque tipo di "rivoluzione" e, in particolare, dinanzi alla "rivoluzione digitale"

tracciarsi nel riconoscimento dell'essenzialità dell'apporto "emotivo" al processo decisionale, di cui soltanto taluni segmenti, magari specificamente connotati dalla necessità di calcoli probabilistici e statistici, potranno essere rimessi all'elaborazione di "macchine" ben informate[75].

In definitiva, è proprio nella centralità della cc.dd. «giustizia poetica», nella presa d'atto, cioè, che «per essere pienamente razionali, i giudici devono anche essere capaci di fantasia e di simpatia», e «migliorare», dunque, «non solo le loro capacità tecniche, ma anche la loro capacità di essere umani»[76], che è dato rintracciare uno dei presidi più potenti, non soltanto dello *status* di presunto innocente di ciascun soggetto coinvolto nella vicenda penale ma, al contempo, della stessa dignità di quest'ultimo[77]: soltanto laddove venga giudicato da un suo simile, con una decisione davvero suscettibile di ampia critica, il destinatario dell'addebito sfugge al rischio di un sindacato depersonalizzato e depersonalizzante che smentirebbe l'essenza stessa del giudizio[78].

Né il diritto in genere, né il diritto processuale penale in particolare, possono

---

BARICCO, *The Game*, Torino 2018, 10-11: «Poiché le riesce più facile percepire il mondo quando il mondo procede a una velocità misurata, lo rallenta; poiché in generale le è più congeniale il gioco di difesa, dà il meglio in presenza di nemici e catastrofi incombenti; poiché in generale non ha predisposizione per il gioco d'attacco, teme il futuro».

[75] Deve ad esempio leggersi in quest'ottica di "sussidio" (...e non di surroga) allo svolgimento della funzione giurisdizionale classicamente intesa, la previsione dell'ordinamento giudiziario spagnolo giusta la quale «*l*os procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley » (art. 230 comma 4 della Ley Orgánica 6/1985 del Poder Judicial come modificato dall'art. 32 della Ley Orgánica 7/2015). Per un'interessante ricostruzione delle posizioni dottrinali registrate in merito alla c.d. *"informatica juridica procesal decisional"*, ovvero all'ipotizzabilità di una completa automatizzazione delle decisioni giudiziali, vd. di nuovo PREZ-LUÑO ROBLEDO, *El procedimiento de* habeas data, cit., 44 ss.

[76] Così NUSSBAUM, *Giustizia poetica. Immaginazione letteraria e vita civile*, (a cura di Greblo), Milano-Udine 2012, 171-172.

[77] «La tecnologia non potrà mai sostituirsi alla giustizia, perché carattere ontologico di quest'ultima è quello di dialogare con le passioni umane»: così, anche da ultimo GARAPON nell'intervista di Novi, *Il computer cambia la giustizia, ma non sarà né giudice né avvocato*, in *Il Dubbio*.

[78] Più in generale, con la consueta capacità di pre-vedere le ricadute delle innovazioni scientifiche e tecnologiche sulle libertà e sui diritti delle persone, a proposito del rapporto tra *data mining* e decisione, RODOTÀ (*Il diritto di avere diritti*, cit., 401) esortava a sottrarre i singoli a quel pericoloso processo di «spersonalizzazione» nel quale «scompare la persona del decisore, sostituito appunto da procedure automatizzate; e scompare la persona in sé considerata, trasformata in oggetto di poteri incontrollabili». Di recente, con non minore incisività, osserva LUCIANI (*La decisione giudiziaria robotica*, in *Rivista AIC* 2018, n. 3., 893): «...noi giuristi possiamo controllare (e criticare) la cultura di un giudice ben più facilmente di quanto possiamo fare con la cultura di un ingegnere, di un matematico, di un programmatore. Per esser chiari: se devo scegliere qualcuno di cui non fidarmi, personalmente, scelgo il giudice. E scelgo che sia un essere umano. Umano e consapevole dell'importanza, certo, ma anche dei limiti, della sua funzione».

smarrire la propria *vis* ed il significato profondo della loro missione delegando a quanto "tecnologicamente possibile" il dettato di ogni regola. E proprio nella prospettiva di sollecitare i decisori politici, i giuristi e i professionisti tutti della giustizia ad abbandonare la sostanziale inerzia che finora li ha contraddistinti, ed a governare, piuttosto che a "reattivamente" subire, i complessi fenomeni sottesi alla "rivoluzione digitale", devono leggersi le iniziative di recente assunte da prestigiose istituzioni quali la Commissione europea per l'efficacia della giustizia del Consiglio d'Europa (CEPEJ) da una parte, e la Commissione Europea dall'altra. Comune il loro obiettivo: quello di assicurare un quadro giuridico ed etico adeguato ad una strategia di sviluppo e di utilizzazione dell'intelligenza artificiale (anche) nell'ambito dei sistemi giudiziari. Altrettanto condiviso, purtroppo, il profilo di debolezza: entrambi i documenti adottati dai richiamati organismi – rispettivamente la Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi di giustizia penale e in ambiti connessi, emanata il 4 dicembre 2018[79], e la bozza di Linee guida di tipo etico per un'intelligenza artificiale affidabile, resa pubblica il 18 dicembre dello stesso anno[80] – sono tipici strumenti di *soft law* e, in quanto tali, difettano di vincolatività[81]. La loro efficacia concreta, in poche parole, è rimessa alla volontaria adesione degli attori pubblici e, non meno significativamente, a quella delle multinazionali tecnologiche *naturaliter* incaricate della progettazione e dell'implementazione dei congegni e dei servizi di IA.

Fatta, però, questa doverosa premessa, non si può disconoscere il valore senza dubbio "pionieristico" di questi strumenti di fonte sovranazionale, nei quali per la prima volta vengono messi a fuoco i principi sostanziali e metodologici da applicarsi nello sviluppo di sistemi intelligenti. *Fil rouge* di ciascun documento è la centralità dell'essere umano nel rapporto con l'intelligenza artificiale: anche e soprattutto quando entrano in gioco gli algoritmi, la tutela della dignità e delle libertà umane non può essere né pretermessa né posposta.

Con particolare attenzione, poi, al miglioramento dell'efficienza e della qualità della giustizia tramite l'impiego, appunto, di strumenti e di servizi di IA di cui la *Carta* si fa espressa promotrice, sono cinque i principi specificamente

---

[79] Il testo integrale è reperibile all'indirizzo *www.rm.coe.int*.

[80] Il testo – elaborato da un gruppo di 52 esperti provenienti dall'industria privata, dall'accademia e dalle istituzioni pubbliche (*High-Level Expert Group on Artificial Intelligence*) – è stato sottoposto a consultazione pubblica per un mese dalla sua pubblicazione, ed è reperibile all'indirizzo *www.ec.europa.eu.*

[81] Per le caratteristiche di questo meccanismo di normazione "non ordinario", cui si fa sempre più frequentemente ricorso anche nell'ambito del diritto processuale penale interno, cfr. BERNARDI, *Sui rapporti tra diritto penale e soft law*, in *Riv. it. dir. proc. pen.* 2011, 2, 536 ss. e TRAPELLA, *Brevissimo viaggio nel* soft-law *processuale, ovvero il giudizio penale al tempo dei protocolli*, in *Cass. pen.* 2018, 1, 4013 ss.

enunciati: si muove dal rispetto dei diritti fondamentali, per poi passare al principio di non discriminazione, al principio di qualità e sicurezza, a quello di trasparenza, imparzialità e correttezza, per chiudere, infine, col principio del c.d. "controllo dell'utente".
Ciò che emerge fin da subito, anche da una rapida lettura delle note esplicative predisposte dalla Commissione per ciascuna delle richiamate garanzie, è la valorizzazione "spinta" di un approccio attento alla "legalità" del procedere e del decidere, piuttosto che al risultato in sé. Ne discendono, *a fortiori*, non poche conferme alle sensazioni di disagio e di imbarazzo già (più o meno espressamente) palesate nel corso della nostra analisi.
Senza bisogno di addentrarsi in un esame puntuale delle singole enunciazioni della *Carta*[82], basta rivolgere lo sguardo all'indietro, a taluna delle questioni già trattate, per avere contezza degli attriti che inevitabilmente si determinano tra i valori da ultimo espressi e gli orizzonti (non di rado distopici) dischiusi da una rincorsa all'utilizzo delle nuove tecnologie (finora) non accompagnata da uno studio serio e davvero multidisciplinare delle trasformazioni che esse possono ingenerare (anche e soprattutto) nel corpo dei diritti degli individui.
Così, come potrebbe non allarmare la distanza che intercorre, da un lato, tra la proclamata necessità che le informazioni trattande – peraltro esclusivamente ricavabili da fonti certificate – siano preservate nella loro integrità in tutte le fasi del trattamento[83]; che le tecniche di processazione impiegate siano accessibili, conoscibili e verificabili *ab externo*[84], e, dall'altro, la rilevata laconicità del legislatore europeo proprio negli snodi fondamentali della Direttiva 2016/681/UE?[85] Una Direttiva che – si noti bene – non soltanto non si preoccupa di rendere ostensibili i "criteri di rischio" sulla scorta dei quali le competenti autorità nazionali dovrebbero espletare l'analisi automatizzata dei dati PNR relativi a soggetti che, per di più, non risultano gravati da elementi indizianti, ma che nemmeno circoscrive il perimetro dei *database* qualitativamente adeguati per la necessaria attività di confronto[86]...

---

[82] Per cui si rinvia ai lavori di BARBARO, *Cepej, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (AI) nei sistemi giudiziari*, in *www.questionigiustizia.it*; e QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali ed informatiche*, in *Legisl. pen.*, 2018, 1 ss.
[83] Vd. *Carta Etica*, cit., 8.
[84] Vd. *Carta Etica*, cit., 9. Parla di «completa trasparenza tecnica, accompagnata da un'esplicazione del processo computazionale in linguaggio accessibile e chiaro» QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali ed informatiche*, cit., 8.
[85] Vd. *supra* nel testo *sub* § 3.
[86] Cfr., al riguardo, la genericità della locuzione utilizzata tanto dalla Direttiva (art. 6 § 3 lett. *a*), quanto

Non solo: preso atto della capacità, peraltro singolarmente elevata in materia penale, di talune applicazioni a disvelare le discriminazioni esistenti aggregando o classificando i dati relativi a persone o a gruppi di persone[87], come può ritenersi compatibile il rispetto del principio di non discriminazione – vale a dire dell'obbligo, facente capo sia agli attori pubblici che a quelli privati, di garantire che simili applicazioni non riproducano o comunque non aggravino dette diseguaglianze o non conducano, comunque, ad analisi deterministiche – con l'utilizzo di formule algoritmiche non trasparenti e, in quanto tali, non verificabili nella loro accuratezza, come quelle per l'appunto sottese alle citate valutazioni automatizzate di rischio della Direttiva 2016/681/UE?

Del resto, se l'alea di effetti così discutibili è in qualche modo ancora "accettabile" in un'ottica, per così dire, "meramente" preventiva[88] (...ammesso e non concesso che la tentazione di utilizzare anche in sede processuale i dati raccolti trovi "argini" giuridici sufficientemente saldi[89]), essa diviene del tutto intollerabile nello spettro del processo penale vero e proprio, e della deliberazione in particolare.

Fatalmente, il filo del discorso si riannoda al punto in cui si era interrotto per dar conto delle direttive stilate a livello sovranazionale.

Difatti, a corroborare gli argomenti di caratura costituzionale già spesi a proposito dell'insostenibilità di un processo decisionale rimesso a reti neurali e modelli che, almeno *rebus sic stantibus*, non sono in grado di compartecipare la "ricchezza" dell'intelligenza umana e la varietà delle piattaforme cognitive a disposizione del "giudice uomo" [90], sopraggiungono gli stessi moniti della *Carta* che, appellandosi al citato principio di non discriminazione, mette anzitutto in guardia dal tributare un crisma di neutralità ai sistemi computazionali ad esempio utilizzabili per la stima del rischio di recidiva o della pericolosità sociale degli accusati. All'uopo viene fatto espresso richiamo alla vicenda COMPAS, ed alla denuncia di Propublica giusta la quale il *software* in questione "misurava" come due volte più probabile che gli uomini di colore commettessero reati rispetto ai bianchi; immagazzinando dati giudiziari (*i.e.*: statistiche degli uffici di polizia e precedenti giurisprudenziali), l'algoritmo –

---

dal decreto legislativo di attuazione interna (art. 8 co 1 lett. *a*).

[87] Vd. *Carta Etica*, cit., 7.

[88] Tratta degli strumenti di "*predictive policing*" l'Appendice I, § 7.1 (*Tools used by investigative authorities before the criminal trial*) della *Carta Etica*.

[89] ...del che giustamente dubita PULITO, *Il trattamento dei dati personali in ambito penale e l'uso del* passenger name record *per contrastare il terrorismo e altri gravi reati*, cit., 1149.

[90] ...anche se nulla esclude che l'avanzamento degli studi possa condurre ad un simile risultato: cfr., al riguardo, i "laici" rilievi di FERRUA, *La prova nel processo penale, Struttura e procedimento*, volume I, Torino 2017, 186.

sottolinea al riguardo la *Carta* della CEPEJ non faceva che riprodurre e ipostatizzare una peculiare "fragilità" sociale ed economica di certi gruppi di popolazione[91], fragilità che ovviamente nulla aveva ed ha a che vedere con un'irrealistica tendenza criminogena "per natura" o "per razza".
Accanto agli *alert* concernenti l'immissione di *bias* preesistenti, il documento stilato dai rappresentanti dei 47 Stati aderenti al Consiglio d'Europa, rafforza le ragioni di cautela che devono presidiare l'introduzione di detta tecnologia trasformativa (l'IA, appunto) nelle pieghe della giustizia penale, dando conto di altri significativi condizionamenti che potrebbero inficiare il processo decisionale. Tra essi, più in dettaglio, la violazione della parità delle armi di cui all'art. 6 CEDU a causa della c.d. *knowledge impairment* che inevitabilmente condiziona le parti dinanzi agli *arcana* algoritmici; e la tentazione (tutt'altro che irrealistica) del giudice di aderire passivamente alla dimensione "formale" propria della sequenza alfanumerica utilizzata, al fine di sottrarsi all'addebito di essere intervenuto in forma troppo "creativa" nel definire i presupposti rilevanti per l'affermazione o meno della responsabilità del prevenuto[92].
Piuttosto, un'adeguata conciliazione tra l'esigenza di non sconfessare *a priori* le indicazioni derivanti dall'algoritmo e il rischio di una supina accettazione delle stesse, potrebbe consistere nel dotare il giudice di un potere valutativo effettivo in ordine alle stesse basi di riferimento su cui l'algoritmo è stato progettato, e dunque, in definitiva, in merito all'algoritmo medesimo; una prospettiva dischiusa, per l'appunto, dalla stessa *Carta Etica* nel momento in cui si preoccupa di declinare la garanzia in virtù della quale gli utilizzatori della IA debbano essere "attori informati" e per tale ragione in grado di esplicare un controllo sulle soluzioni "artificialmente" prodotte[93].
Sia pure scontando il carattere provvisorio di ogni sintesi finale, l'orizzonte aperto dalla scelta di promuovere l'utilizzazione dell'IA nei sistemi giudiziari, non si presta, come già anticipato, ad una chiave di lettura unilaterale, vuoi orientata in chiave critica, vuoi, all'opposto, incondizionatamente favorevole[94]. Si tratta, infatti, di una tematica che *ab origine*, per così dire, è contrassegnata da un accentuato livello di complessità: tale essendo quello che ne situa la dimensione funzionale in un "crocevia" di rapporti e di interazioni tra campi

[91] Cfr. Appendice I, § 7.2 (*Tools during the criminal trial*) della *Carta Etica*.
[92] Vd. Appendice I, § 7.3. (*The challenges of "prediction" in criminal matters*) della *Carta Etica*. In termini più estremi, sui rischi di cui potrebbe esser volano una, per così dire, "certezza giuridica robotica" (malamente) intesa alla stregua di puro "vincolo al precedente giurisprudenziale", si vedano le ricche riflessioni di LUCIANI, *La decisione giudiziaria robotica*, cit., 886 ss.
[93] Così, appunto, il principio dell'"*under user control*" di cui alla *Carta Etica*, cit, 5.
[94] «*Il ne faut pas fétichiser la tecnique*» ci ricordano GARAPON, LASSÈGUE, *Justice digitale. Révolution graphique et rupture anthropologique*, cit., 122.

del sapere insuscettibili, oramai, di venire governati secondo quelle logiche di separatezza e di autosufficienza sistematica ereditate da una pur gloriosa tradizione. In un simile contesto, si atteggia come ineludibile la predisposizione di un opportuno "canale di comunicazione" e di virtuosa influenza tra etica, diritto ed innovazioni tecnologiche: la prima ed il secondo, quali garanzie indefettibili della dignità umana e di sviluppo delle procedure di elaborazione delle decisioni giudiziarie alla luce dei principi consolidati; le ultime, come "ponte" gettato verso un futuro auspicabilmente incentrato su di una maggiore efficienza operativa.

Perché – ed è verità, questa, che oggi più che mai deve ritenersi insuscettibile di ritrattazioni o, comunque, di letture "al ribasso" – il *welfare* della giustizia penale, la sicurezza e il benessere del sistema giustizia, non possono essere riduttivamente intesi alla stregua di pura *performance*, ossia di mere prestazioni di risultato, quantificabili in aride percentuali o in sterili rapporti statistici.

La *governance* dell'informatica e, più in generale, degli strumenti di IA al servizio della soluzione giuridica, deve necessariamente passare attraverso una massimizzazione delle risorse[95] che non sia mai disgiunta, però, da una salda strutturazione valoriale, ossia da un'impostazione che consenta l'utilizzo di grandi moli di informazioni e la semplificazione di complesse procedure decisorie nel rispetto, sempre, dei canoni fondanti il giusto processo. In definitiva, una giustizia *as fairness*, non una giustizia *as fitness*[96].

[95] ... a cui – si osservi – fanno da "farsesco controcanto" le clausole di invarianza finanziaria inserite alla stregua di postilla e sigillo finali nei diversi decreti sopra richiamati e promulgati in attuazione della *policy* europea. Così, a dimostrazione della scarsa attitudine ad affrontare *funditus*, da parte del legislatore italiano, tematiche tanto impegnative, basterà tener conto dell'art. 50 d.lgs. 51/2018 o dell'art. 27 d.lgs. 53/2018, entrambi significativamente rubricati «*Clausola di neutralità finanziaria*».

[96] L'efficace proposizione antitetica è presa in prestito da GARAPON, LASSÈGUE, *Justice digitale. Révolution graphique et rupture anthropologique*, cit., 315 ss. i quali, a loro volta, la mutuano, per una parte almeno, dal celebre contributo di J. RAWLS, *Justice as fairness. A Restatement*, Harvard 2001.