

ARIANNA VEDASCHI, CHIARA GRAZIANI
SICUREZZA PUBBLICA,
DIRITTI E TECNOLOGIA:
LE SFIDE DELL'INTELLIGENZA ARTIFICIALE

1. *Considerazioni introduttive*

Le sfide alla sicurezza poste dal terrorismo internazionale di matrice jihadista sono una costante del ventunesimo secolo¹. I noti e tragici eventi dell'11 settembre 2001 hanno rappresentato l'inizio di una minaccia che non ha ancora cessato di mettere a rischio, insieme alla sopravvivenza – fisica – delle persone, la tenuta delle garanzie alla base delle democrazie c.d. mature e, in ultima analisi, la *rule of law*.

L'emergenza terroristica risulta talmente pervasiva che, a livello teorico-dottrinale, il concetto di sicurezza – prima del 2001 pacificamente considerato come un interesse collettivo che, in via eccezionale e temporanea, poteva legittimare limiti alle libertà e ai diritti dei cittadini² – è stato oggetto di una significativa rielaborazione. Vi è, in dottrina, chi oggi interpreta la sicurezza alla stregua di un diritto soggettivo della persona³, da bilanciare con gli altri diritti e libertà; e addirittura chi la fa assurgere a rango costituzionale, come se si trattasse di un principio “supremo”, preconditione per il godimento di tutti gli altri diritti e libertà⁴. Secondo questa posizione, la sicurezza non potrebbe entrare in un'eventuale operazione di bilanciamento, in quanto si trova al di là e al di sopra degli interessi da bilanciare.

-
- 1 V., sullo sviluppo delle *counter-terrorism measures* negli ultimi venti anni e le relative questioni giuridiche, A. Vidaschi, K.L. Scheppele (a cura di), *9/11 and the Rise of Global Antiterrorism Law. How the UN Security Council Rules the World*, Cambridge 2021.
 - 2 Sul punto v., per tutti, A. Pace, *Il concetto di ordine pubblico nelle Costituzione italiana*, in *Archivio giuridico “Filippo Serafini”*, n. 1, 1963, pp. 111 ss.
 - 3 G. de Vergottini, *La difficile convivenza fra libertà e sicurezza*, Relazione al convegno dell'Associazione Italiana dei Costituzionalisti, 2003; T.E. Frosini, C. Bas-su, *La libertà personale nell'emergenza costituzionale*, in A. Di Giovine (a cura di), *Democrazie protette e protezione della democrazia*, Torino 2005, pp. 77 ss.
 - 4 V., in tal senso, G. Cerrina Feroni, G. Morbidelli, *La sicurezza: un valore super-primario*, in *Percorsi costituzionali*, n. 1, 2008, pp. 31 ss.

Tale “rivoluzione” nelle elaborazioni teoriche del concetto di sicurezza⁵ – sebbene non si possa dimenticare che vi è chi continua a leggerla, anche nel c.d. *post-9/11*, come interesse collettivo che, eccezionalmente, giustifica limiti all’esercizio delle libertà⁶ – è dovuta, in buona parte, alla presa di coscienza della peculiarità della “inedita” minaccia⁷ che a far tempo del 2001 preoccupa la società civile. Il terrorismo internazionale, infatti, si caratterizza per l’agire “a macchia di leopardo”, data l’imprevedibilità nella localizzazione dei suoi attacchi, che si aggiunge all’incertezza nell’*an*, nel *quando* e nel *quomodo* degli attentati. Ciò contribuisce a creare, nella società civile, una diffusa percezione di insicurezza⁸, che richiede, sul piano teorico, una rilettura dell’idea di sicurezza e, sul piano pratico, l’adozione di misure comportanti significative limitazioni di basilari diritti, “vittime collaterali” della *war on terror* e delle conseguenti esigenze securitarie.

Le misure antiterrorismo si connotano, da un lato, per un necessario approccio preventivo (il che comporta l’anticipazione della soglia di intervento rispetto alla commissione del fatto) e, dall’altro, per l’efficienza della risposta, con riguardo alla tempistica. La necessità di prevenzione combinata a quella di efficienza implica che, almeno in teoria, i sistemi automatizzati basati sull’intelligenza artificiale (c.d. algoritmi intelligenti) appaiano i “candidati ideali” a supportare l’azione del potere pubblico a tutela della sicurezza dello Stato e dei suoi cittadini. Tuttavia, i *caveat* di natura giuridica sono ancora molti e meritano considerazione tanto dalla prospettiva dottrinale quanto da quella pratica.

Le riflessioni che seguono si propongono, in primo luogo, di approfondire l’interazione tra intelligenza artificiale e la sicurezza pubblica, anche con esemplificazioni puntuali di come la prima possa essere funzionale alla seconda e, nello specifico, alle *counter-terrorism measures* (par. 2). L’indagine proposta individua, dunque, i principi e i diritti potenzialmen-

5 Per un’analisi approfondita, anche dal punto di vista giuridico-filosofico, delle nuove interpretazioni del concetto di sicurezza, v. M. Barberis, *Non c’è sicurezza senza libertà. Il fallimento delle politiche antiterrorismo*, Bologna 2016.

6 A. Pace, *Libertà e sicurezza. Cinquant’anni dopo*, in *Diritto e società*, n. 2, 2013, pp. 177 ss.

7 Sulle evoluzioni della minaccia terroristica, v. A. Vidaschi, *Da al-Qā’ida all’IS: il terrorismo internazionale “si è fatto” Stato?*, in *Rivista trimestrale di diritto pubblico*, n. 1, 2016, pp. 41 ss.

8 Sul ruolo della percezione di insicurezza degli individui nella configurazione delle politiche antiterrorismo da parte del potere pubblico, v. A. Vidaschi, *Seguridad y libertad en tiempo de terrorismo internacional. Entre percepción de inseguridad y populismo*, in J.J. Fernández Rodríguez (coord.), *Democracia y seguridad: respuestas para avanzar en el sistema público*, Valencia 2021, pp. 195 ss.

te intaccati dall'applicazione di tali strumenti di tecnologia avanzata, con particolare riguardo alle politiche antiterrorismo (par. 3). Anzi, sull'assunto che alcuni di questi diritti sono limitabili a condizione che venga rispettato il principio di proporzionalità, la domanda di ricerca che si vuole affrontare è quella di valutare se gli "indicatori" enucleati dalle corti per verificare la compatibilità con il *proportionality test* siano effettivamente rispettati dall'uso dell'intelligenza artificiale (par. 4). Orbene, dopo aver rilevato che molti di questi *standards* sono messi perlomeno sotto *stress* dall'algoritmo intelligente, si valutano le possibili soluzioni, così da offrire, nella parte conclusiva, spunti relativi ad eventuali "cambi di rotta" che, nel mettere a punto o quantomeno nell'aggiornare le misure antiterrorismo basate sull'intelligenza artificiale, i legislatori potrebbero intraprendere nell'intento di garantire la migliore interazione tra i tre fattori sicurezza-diritti-tecnologia alla base di questo studio.

2. Sicurezza pubblica, counter-terrorism measures e intelligenza artificiale

"The Government [...] cannot wait for terrorist disaster to strike before taking necessary steps to prevent it"⁹ asseriva Lord Bingham in una nota decisione del 2004, in cui l'Appellate Committee della House of Lords britannica si pronunciava sulla compatibilità con lo Human Rights Act 1998 di talune contestate *counter-terrorism measures*. Da questa statuizione risulta, in tutta evidenza, l'indole *preventiva* che, come detto in precedenza, connota le misure antiterrorismo.

Le indubbie capacità *predittive* delle applicazioni di intelligenza artificiale ben sembrano allora rispondere alle esigenze di prevenzione insite nell'azione di *counter-terrorism*. Basti ricordare, a mero titolo di esempio, la capacità degli algoritmi di valutare *in anticipo* il rischio di radicalizzazione, tanto *in uscita* (grazie all'identificazione della narrativa terroristica presente nella rete internet¹⁰) quanto *in entrata* (grazie alla rilevazione e

9 Il riferimento è alla sentenza *A. and others v. Secretary of State for the Home Department* [2004] UKHL 56 (c.d. caso *Belmarsh*).

10 Si veda, a tal proposito, il recente Regolamento (UE) 2021/784, rubricato "Regolamento relativo al contrasto della diffusione di contenuti terroristici online". Questa fonte, nel tentare l'armonizzazione delle discipline degli Stati in materia di rimozione dei contenuti terroristici *online* con particolare riguardo alla regolamentazione dell'inevitabile interazione tra potere pubblico e soggetti privati, non pone però norme specifiche circa l'utilizzo degli strumenti tecnologici. Di conseguenza, il ricorso a tecniche di intelligenza artificiale risulta, oltre che assai probabile, sostanzialmente non regolato.

all'analisi algoritmica dei metadati concernenti le ricerche in rete al fine di identificare l'adesione all'ideologia di matrice terroristica¹¹). Anzi, l'esame dei dati (in particolare, quelli c.d. biometrici, tra cui i caratteri del volto, le impronte digitali, il timbro di voce) consente di rilevare il rischio che in un dato luogo (pubblico) avvenga un attacco terroristico o comunque un evento che ponga a serio rischio la sicurezza dei presenti. Tale valutazione è resa possibile dal *match* dei dati biometrici delle persone presenti, c.d. riconoscimento facciale¹².

Pertanto, sul presupposto che l'azione preventiva è essenziale nell'attività di contrasto al terrorismo internazionale di matrice jihadista, il ricorso all'intelligenza artificiale è necessario. In effetti, in questo tipo di crimini, molto spesso la morte suicida del terrorista impedisce un'azione efficace sul piano special-preventivo, giacché non si può punire il responsabile con l'armamentario classico del diritto penale. Dunque, la sola opzione utile in campo è quella di anticipare (*rectius*, prevenire) l'azione per evitarla, piuttosto che punirne il responsabile. Vieppiù, sul piano generale, la capacità di *prevenire* attacchi terroristici può funzionare come utile "antidoto" alla percezione di insicurezza che dal 9/11 serpeggia nella società civile.

Un altro aspetto, peraltro intrinsecamente collegato al carattere preventivo, che lega l'intelligenza artificiale alle misure antiterrorismo, è la capacità di contenere i tempi.

A tal riguardo, i c.d. *big data* che "alimentano" gli algoritmi intelligenti, funzionando come *input*, consentono di raccogliere, processare ed analizzare un'enorme quantità di informazioni, per di più ad una velocità non comparabile a quella del più efficiente operatore umano. Pertanto, l'intelligenza artificiale offre grandi vantaggi in termini di *efficacia* relazionata al *timing*. In altre parole, l'algoritmo pare essere un "giocatore imbattibile" nel tempismo dell'azione di contrasto.

Quanto detto sinora sembra evidenziare l'essenzialità dell'intelligenza artificiale nell'ambito delle politiche antiterrorismo, soprattutto in una so-

11 A tal proposito, si può richiamare il c.d. metodo *redirect*, impiegato da Google per identificare utenti che, per i loro *patterns* di ricerca in internet, si configurano come ad alto rischio di radicalizzazione. Questi utenti vengono immediatamente reindirizzati su pagine di c.d. contronarrativa, ossia contenenti informazioni tese a distoglierli dal proposito di aderire ad organizzazioni di stampo terroristico.

12 V., sui problemi giuridici posti dagli algoritmi di riconoscimento facciale o comunque biometrico, A. Pin, 'A Novel and Controversial Technology.' *Artificial Face Recognition, Privacy Protection, and Algorithm Bias in Europe*, in *William & Mary Bill of Rights Law Journal*, vol. 30, n. 3, 2022, pp. 291 ss.

cietà, come quella del ventunesimo secolo, ampiamente “digitalizzata”¹³. Tuttavia, non è scontato, almeno nel sistema di tutela dei diritti e delle libertà proprio delle democrazie c.d. avanzate, l’apparente sillogismo: poiché il *counter-terrorism* richiede capacità preventiva; e dato che l’intelligenza artificiale garantisce il carattere preventivo dell’azione di contrasto; allora, gli strumenti di intelligenza artificiale sono la soluzione ottimale da impiegare nella battaglia contro il terrorismo internazionale.

3. *Questioni giuridiche e criticità dell’impiego dell’intelligenza artificiale nel counter-terrorism*

Si è appurato che non sono né poche né marginali le criticità dell’azione dell’intelligenza artificiale nell’impatto sui diritti e sulle libertà¹⁴, anzi persino basilari principi alle fondamenta della *rule of law* ne risultano intaccati. Senza pretesa di esaustività, da questa prospettiva sembra utile individuare ed esaminare almeno tre delle principali questioni controverse, ovverosia l’impatto dell’intelligenza artificiale sul principio di non discriminazione, sulla *privacy* e sulla protezione dei dati personali – che può persino incidere sul principio di presunzione di innocenza –, nonché il rischio di sproporzionate limitazioni della libertà di espressione.

In primo luogo, focalizzando l’attenzione sul principio di non discriminazione, affinché possano funzionare, tutti gli algoritmi c.d. intelligenti (cioè basati sull’intelligenza artificiale) vengono “allenati” su *sets* di dati. Nel caso in cui, per qualsivoglia ragione – inclusi potenziali *biases* dell’operatore umano, la scarsità delle statistiche a disposizione, la non accuratezza dei metodi di ricerca e analisi delle informazioni – all’algoritmo si fornisca un *set* di dati viziato da pregiudizi, l’algoritmo porrà in essere – in modo purtroppo efficiente – un ragionamento viziato dagli stessi pregiudizi. Ad esempio, qualora un algoritmo volto a riconoscere messaggi terroristici *online* venisse “allenato” su dati parziali, che mostrano solo messaggi

13 V., *ex multis*, P. Passaglia, “Privacy” e nuove tecnologie, un rapporto difficile. Il caso emblematico dei “social media”, tra regole generali e ricerca di una specificità, Relazione al Convegno “El derecho a la intimidad”, Madrid, 22-23 settembre 2016.

14 V., per un’analisi dei rischi dell’intelligenza artificiale di carattere generale e non strettamente focalizzata sulla sicurezza pubblica, A. D’Aloia (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano 2022; A. Simoncini, *L’algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, n. 1, 2019, pp. 63 ss.

in rete di persone immigrate oppure appartenenti ad una data etnia o ancora professanti un determinato credo, quell'algoritmo sarà necessariamente *biased* nei confronti degli immigrati o di persone con un preciso profilo etnico oppure di una certa religione. Vieppiù, esistono casi in cui i *biases* non dipendono da una programmazione "viziata" dell'algoritmo, bensì da peculiarità del suo funzionamento tecnico, sempre però ad alto rischio di discriminazione. Infatti, secondo diversi studi, gli algoritmi usati per il riconoscimento facciale tendono ad aumentare la propria percentuale di errore allorquando operano il *matching* tra visi di persone di colore, rispetto a quando espletano la stessa operazione su volti di soggetti caucasici¹⁵.

In secondo luogo, è opportuno considerare l'impatto che l'intelligenza artificiale può avere sulla *privacy* e sul correlato diritto alla protezione dei dati personali¹⁶. Come già osservato, l'intelligenza artificiale, per "apprendere" al fine di simulare il funzionamento della mente umana, deve lavorare su amplissimi *sets* di dati, molti dei quali risultano riferiti a persone identificate o identificabili e, perciò, configurabili come dati personali. Riprendendo l'esempio dell'algoritmo di identificazione di contenuti terroristici *online*, esso dovrà sottoporre ad analisi un'ingente quantità di messaggi pubblicati sui *social networks*, nonché processare i relativi metadati¹⁷, rappresentati da tutte quelle informazioni che un individuo genera nel pubblicare un certo messaggio su un dato *social network*; si pensi, tra gli altri, all'orario di accesso, alla durata della connessione, alla geolocalizzazione dell'utente e al suo indirizzo IP. Tutti questi dati vengono poi incrociati in maniera automatizzata. Grazie all'opera di *crossing*, l'intelligenza artificiale è in grado di reperire molte più informazioni rispetto a quelle originariamente disponibili, spesso senza che siano osservate le basilari norme in tema di trattamento dei dati personali (come l'ottenimen-

15 T. Gebru et al., *Saving face: Investigating the ethical concerns of facial recognition auditing*, in AIES '20: *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2020, pp. 145 ss.

16 Dal punto di vista dottrinale, vi sono diverse posizioni circa l'autonomia (o meno) della *data protection* rispetto al più risalente riconoscimento del diritto alla *privacy*. V., sulle diverse posizioni, S. Rodotà, *Il diritto di avere diritti*, Roma-Bari 2012, p. 397 (il quale legge la *data protection* come dimensione "dinamica" del diritto alla *privacy*); C. Dockesey, *Four Fundamental Rights: Striking the Balance*, in *International Data Privacy Law*, vol. 6, n. 3, 2016, pp. 195 ss. Sull'impatto dell'intelligenza artificiale su *privacy* e *data protection*, T.E. Frosini, *La privacy nell'era dell'intelligenza artificiale*, in *DPCE Online*, n. 1, 2022, pp. 273 ss.

17 A. Vendaschi, V. Lubello, *Data retention and its implications for the fundamental right to privacy. A European perspective*, in *Tilburg Law Review*, vol. 20, n. 1, 2015, pp. 14 ss.

to del consenso del *data subject* o il principio di minimizzazione del trattamento). Non è neppure escluso che l'incrocio dei dati comporti la profilazione dell'utente, non solo quello "a rischio" di radicalizzazione o di altre condotte pericolose, ma anche di qualsiasi persona dedita a "navigare" in rete. Quasi scontato è allora rimarcare che tale generalizzata profilazione potrebbe comportare rilevanti problemi sia sul versante della protezione dei dati sia su quello della presunzione di innocenza, principio alla base dello stato di diritto.

Infine, molto spesso le tecniche di intelligenza artificiale vengono utilizzate a fini di sorveglianza di massa. Emblematica è la legge francese n. 2015-912 (c.d. *loi sur le renseignement*)¹⁸, che permette ai servizi di *intelligence* di utilizzare i c.d. *black boxes*¹⁹ per esaminare i metadati delle comunicazioni dei cittadini francesi per via telefonica e informatica, in modo da intercettare eventuali utenti sospetti. Ancora una volta, l'applicazione indiscriminata di questi mezzi di prevenzione comporta non pochi rischi. In prima battuta, potrebbe innescarsi un generalizzato *chilling effect*, giacché gli utenti di telefonia e internet, consapevoli di essere sorvegliati, potrebbero essere poco inclini a manifestare liberamente il proprio pensiero, a prescindere dal rilievo penale delle loro esternazioni. In seconda battuta, si pensi al caso, evidenziato in precedenza, dell'algoritmo che identifica al fine di rimuovere i messaggi terroristici *online*. Qualora la rimozione risultasse sproporzionata, se non addirittura errata, assodato che il messaggio postato *online* costituiva legittima espressione di un orientamento politico o religioso, senza esporre ad alcun rischio la sicurezza pubblica, vi sarebbe una (illegittima) interferenza nella libertà di espressione.

Alla luce di questi esempi, che denunciano i limiti dell'intelligenza artificiale, assai pericolosi soprattutto per il contesto di riferimento, sembra opportuno riflettere sulla loro portata così da ponderare l'impiego degli algoritmi.

Si è appena dimostrato che, pur al nobile fine di proteggere la sicurezza pubblica, non pochi diritti (*privacy*, *data protection*) né marginali libertà (libertà di espressione) vengono sottoposti a tensione dai meccanismi automatizzati (dal riconoscimento facciale alla sorveglianza algoritmica). Anzi, si è notato che questi avanzati (al punto da essere definiti intelligenti)

18 Su questa legge, peraltro adottata nel corso del regime dello stato di urgenza dovuto all'emergenza terroristica, v. O. Pfersmann, *L'état d'urgence: la petite exception en dehors de la grande Constitution*, in *Democrazia e sicurezza*, 2016, pp. 3 ss.

19 Si tratta di algoritmi molto avanzati, in grado di produrre un *output*, dato un certo *input*, i cui processi logici non sono interamente conoscibili neppure a chi ha programmato l'algoritmo, visto l'alto grado di autonomia della macchina.

strumenti tecnologici arrivano persino ad incidere su principi cardine delle democrazie avanzate (quali quelli di non discriminazione, presunzione di innocenza, ecc.). D'altra parte, anche a restare sulla posizione classica del concetto, quello della sicurezza è annoverabile tra gli interessi collettivi meritevoli di tutela e, come tale, può legittimare la limitazione di quei diritti ritenuti non assoluti. Di qui la sfida per i legislatori, in via fisiologica, di trovare il punto di equilibrio tra le esigenze della sicurezza pubblica e la compressione delle libertà personali. Punto di equilibrio sottoposto, in via patologica, al vaglio delle corti, che sovente, nel corso del tempo, hanno provato a valutare le *counter-terrorism measures*, incluse quelle basate su forme più o meno avanzate di tecnologia, alla luce del principio di proporzionalità. Nell'applicare il *test* di proporzionalità, i giudici, soprattutto sovranazionali (la Corte di giustizia dell'Unione europea e la Corte europea dei diritti dell'uomo), hanno, negli anni, elaborato indicatori, utili appunto a testare se le restrizioni adottate in nome della sicurezza e basate su tecnologie avanzate fossero proporzionate allo scopo perseguito. Nel paragrafo successivo si vuole indagare sull'*an* e sul *quomodo* questi *standards* siano messi sotto *stress* dagli attuali utilizzi dell'intelligenza artificiale a fini di antiterrorismo.

4. *Intelligenza artificiale e counter-terrorism alla prova del proportionality test*

Al fine di verificare il rispetto del principio di proporzionalità da parte di misure antiterrorismo che implicano l'uso di strumenti tecnologici, i principali *standards* elaborati dalle corti sovranazionali possono essere individuati nella necessità di una base giuridica chiara, nella precisione del *drafting* delle disposizioni, nella presenza di *oversight* da parte di un organo indipendente, chiamato a valutare l'effettivo bisogno di applicare le misure di contrasto, e nella possibilità di una eventuale successiva *review* da parte delle corti.

Per quanto concerne la base giuridica, la giurisprudenza costante tanto della Corte di giustizia dell'Unione europea (dal notissimo caso *Digital Rights Ireland*²⁰ in poi) quanto della Corte europea dei diritti dell'uomo (si pensi, da ultimo, alla sentenza del 2021 *Big Brother Watch v. UK*²¹) sotto-

20 European Court of Justice, C-293/12, *Digital Rights Ireland*, 8 April 2014.

21 European Court of Human Rights, Grand Chamber, apps. nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch v. the United Kingdom and others*, 25 May 2021.

linea che le limitazioni di diritti e libertà per motivi di sicurezza devono, anzi tutto, fondarsi su una base giuridica, non necessariamente legislativa dal punto di vista formale, ma che abbia requisiti minimi di conoscibilità e pubblicità.

Ebbene, allorquando l'intelligenza artificiale viene utilizzata a fini di tutela della sicurezza, è frequente che la base giuridica manchi. Lacuna questa segnalata, tra gli altri, dal Garante italiano per la protezione dei dati personali. Quest'ultimo, in un parere del 25 marzo 2021²², ha sottolineato l'assenza della base normativa per l'utilizzo di sistemi di riconoscimento facciale in luogo pubblico²³.

Non di rado l'utilizzo di algoritmi tesi all'identificazione di contenuti terroristici (o comunque "pericolosi") sul *web* non è dunque regolato da alcuna fonte normativa. Infatti, sebbene il problema della radicalizzazione *online* e dei relativi strumenti per combatterla sia stato recentemente oggetto di attenzione a livello di Unione europea, con il Regolamento (UE) 2021/784²⁴, tale fonte omette di disciplinare l'*an* e il *quomodo* del ricorso ai meccanismi "intelligenti"²⁵. Di conseguenza, il punto viene implicitamente rimesso alle scelte degli operatori del *web*, i quali godono di una significativa (e forse troppo ampia) discrezionalità.

Strettamente connesso al tema della base giuridica è il secondo "indicatore" menzionato. Tanto per la Corte di Lussemburgo quanto per quella di Strasburgo, la base giuridica è necessaria ma non sufficiente, poiché deve essere scritta in modo chiaro, preciso, tassativo e non ambiguo.

Per varie ragioni, l'impiego di tecniche di intelligenza artificiale applicate alla sicurezza non sempre rende facile il rispetto di questi basilari requisiti. In primo luogo, le norme che riguardano l'uso di tecnologia avanzata vengono spesso volutamente formulate in modo da lasciare margini di discrezionalità ai soggetti "operativi" – organi dell'Esecutivo, servizi di *intelligence*, nonché autorità di *law enforcement*. È emblematico il caso francese, dove il noto meccanismo dei *black boxes* è disciplinato da una legge

22 Garante per la protezione dei dati personali, Parere sul sistema Sari Real Time, 25 marzo 2021 [9575877].

23 Il parere era stato richiesto dal Ministero dell'Interno circa la possibilità di utilizzare Sari Real Time, uno strumento di riconoscimento facciale basato su algoritmi capace di attuare l'analisi e il *matching* in tempo reale di dati biometrici.

24 Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici *online*.

25 V., sul punto, C. Graziani, *Intelligenza artificiale e fonti del diritto: verso un nuovo concetto di soft law? La rimozione dei contenuti terroristici online come casestudy*, in *DPCE Online*, Speciale, 2022, pp. 2037 ss.

formale²⁶, però dal *drafting* vago e generico, il che lascia un ampio margine di azione ai servizi di *intelligence*. Un secondo motivo per cui le basi giuridiche, laddove esistenti, risultano spesso poco chiare è dovuto al fatto che l'algoritmo "intelligente" è normalmente sviluppato e concretamente implementato da un soggetto privato, a cui il potere pubblico si "appoggia" in una sorta di *partnership*²⁷. Si pensi a Facebook, che possiede una propria *policy*, anche piuttosto articolata, in materia di identificazione di contenuti terroristici grazie a strumenti algoritmici; cionondimeno, il punto chiave della stessa, ovvero cosa sia un contenuto "terroristico", non viene mai precisato. A tal riguardo, va detto che la responsabilità della "non definizione" del contenuto terroristico è prima di tutto e soprattutto del potere pubblico, posto che anche a livello internazionale non si è ancora arrivati ad una definizione universalmente condivisa del fenomeno terroristico²⁸.

Il terzo indicatore a cui si è fatto riferimento è l'esistenza di un *oversight* preventivo sulle misure che implicano l'uso di mezzi tecnologici avanzati. L'attività di *oversight*, sempre secondo le corti sovranazionali, può essere svolta da un'autorità giudiziaria o quantomeno da un'autorità amministrativa indipendente.

Orbene, non sempre questo requisito viene rispettato quando i meccanismi di intelligenza artificiale vengono impiegati con lo scopo di tutelare la sicurezza pubblica. Si consideri il riconoscimento facciale. Come ben esemplificato dal caso italiano, spesso l'impiego di questa tecnologia non contempla una base giuridica. Di conseguenza, se non esiste una base giuridica, neppure esiste il vincolo di *oversight* giudiziario o amministrativo. Né queste tecnologie si possono ricondurre alla più ampia disciplina delle intercettazioni, regolate dai codici di procedura penale della gran parte degli ordinamenti democratici con puntuali requisiti procedurali – inclusa la supervisione dell'autorità giudiziaria²⁹.

La mancanza di *oversight* risulta poi di tutta evidenza nel caso della sorveglianza di massa attuata con strumenti algoritmici. A tal proposito, l'esempio francese dei *black boxes* è ancora una volta calzante. Secondo

26 Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

27 Sul tema, C. Graziani, *Removing Terrorist Content Online. The Intersection between the International, Regional, and Domestic Level*, in A. Vidaschi, K.L. Scheppelle (eds.), *op. cit.*, pp. 222 ss.

28 M. Scheinin, *A Proposal for a Kantian Definition of Terrorism. Leading the World Requires Cosmopolitan Ethos*, in A. Vidaschi, K.L. Scheppelle (eds.), *op. cit.*, pp. 15 ss.

29 In Italia, per esempio, le intercettazioni possono essere attuate su disposizione del pubblico ministero previa autorizzazione del giudice per le indagini preliminari. V. art. 267 del codice di procedura penale.

la normativa in vigore, per l'uso di questi algoritmi altamente sofisticati da parte dei servizi di *intelligence* è sufficiente la mera autorizzazione del Primo Ministro, dunque di un organo dell'Esecutivo, privo delle caratteristiche di indipendenza, imparzialità e terzietà che contraddistinguono l'autorità giudiziaria (o, seppur secondo schemi diversi, quella amministrativa indipendente³⁰). Vero è che, sempre nel caso francese, il Primo Ministro, prima di concedere l'autorizzazione, è obbligato ad acquisire il parere della Commission Nationale de l'Informatique et des Libertés – ossia un'autorità amministrativa indipendente che svolge le funzioni di *data protection authority*; tuttavia, questo parere non è vincolante, tant'è che il Primo Ministro può, previa motivazione, discostarsene.

Il quarto *standard* menzionato viene identificato nell'esistenza di un controllo giurisdizionale (*review*) da attuarsi *a posteriori*. In altre parole, secondo la giurisprudenza di Lussemburgo e quella di Strasburgo, deve essere sempre garantita la verifica giurisdizionale successiva qualora la persona a cui viene applicata la misura ritenga che questa sia viziata da profili di illegittimità.

Quando gli strumenti automatizzati vengono in gioco, tale controllo può essere particolarmente arduo. *In primis*, non sempre il meccanismo di funzionamento dell'algoritmo è lineare e intellegibile, il che può rendere complesso un controllo giurisdizionale effettivo. In altri termini, quegli algoritmi – come i *black boxes* – talmente autonomi da arrivare ad un *output* con un *reasoning* non conoscibile neppure da coloro che li hanno programmati potrebbero ostacolare una logica motivazione della sentenza. *In secundis*, funzioni equiparabili a quelle giurisdizionali sono spesso svolte, stando alle *policies* dei vari attori privati, da soggetti né terzi né imparziali. A questo riguardo, può essere menzionato il Facebook Oversight Board, che ha iniziato a lavorare nell'ottobre 2020³¹. Questa “esternalizzazione”, a favore di soggetti legati ad enti privati, di funzioni latamente riconducibili a quella

30 V. A. Patroni Griffi, *L'indipendenza del Garante*, in *Federalismi.it*, 2018, pp. 22 ss.

31 Il Facebook Oversight Board (dal 9 giugno 2022, Meta Oversight Board) è formato da membri (almeno undici) di diverso *background* professionale e di diversa provenienza geografica, così da assicurare l'accuratezza delle decisioni e la rappresentatività del comitato. Esso prevede un meccanismo di nomina dei membri (che restano in carica per tre anni) molto articolato. Infatti, l'azienda Facebook (Meta) seleziona un gruppo di co-presidenti del Board; i co-presidenti selezionano i restanti membri del Board; sull'indipendenza del Board vigila un *trust* creato dallo stesso Facebook (Meta). Sebbene questa complicata procedura di nomina costituisca uno sforzo apprezzabile per assicurare una certa indipendenza rispetto a Facebook (Meta), i risultati non sono certo paragonabili al concetto di indipendenza tradizionalmente proprio dell'organo giudicante.

giurisdizionale getta luce su un processo di progressivo scollamento tra la funzione giurisdizionale in senso oggettivo e l'organo giurisdizionale in senso soggettivo. Lungi dall'essere un fenomeno meramente formale, esso comporta importanti ripercussioni sulle caratteristiche basiche che il diritto costituzionale tradizionale attribuisce all'organo giurisdizionale, quali l'indipendenza, l'autonomia, la terzietà, l'imparzialità³².

Last but not least, i quattro indicatori analizzati sono stati elaborati dalle corti per valutare se le limitazioni di diritti e libertà considerati non assoluti, attuate in nome della sicurezza pubblica con il ricorso a mezzi tecnologici, siano o meno conformi al principio di proporzionalità. Il discorso diviene ancora più complesso quando si parla non più di diritti limitabili (*privacy*, *data protection*, libertà di espressione), ma di principi incompressibili, che dovrebbero anzi fungere da "controlmite" a qualsiasi restrizione. Il riferimento è, prima di tutto, al principio di non discriminazione, potenzialmente impattato dal funzionamento dell'algoritmo. Anche un sistema algoritmico perfettamente normato da una disposizione chiara e precisa, che preveda appropriati controlli *a priori* e *a posteriori*, sarebbe comunque illegittimo se fosse discriminatorio³³.

5. Prospettive di diritto positivo

Lo scenario tratteggiato e i rischi collegati non devono portare il giurista, o comunque il soggetto "non tecnico" in materie come l'informatica e la robotica, a concludere che l'intelligenza artificiale non possa – e non potrà mai – essere utilizzata per contrastare le minacce alla sicurezza. Al contrario, azionato il "livello di allerta", il giurista deve raccogliere la sfida lasciata dall'algoritmo ed elaborare strumenti in grado di mitigare (o perlomeno tenere sotto controllo) i rischi per la *rule of law*.

È in quest'ottica che bisogna chiedersi: fino a questo momento, che cosa è stato fatto in tal senso? Esiste – o è *in fieri* – una regolamentazione giuri-

32 Sull'impatto dell'intelligenza artificiale sui poteri pubblici, v. C. Casonato, *L'intelligenza artificiale e il diritto pubblico comparato ed europeo*, in *DPCE Online*, n. 1, 2022, pp. 169 ss.

33 Questo punto è particolarmente rimarcato nel parere con cui la Corte di giustizia dell'Unione europea, nel luglio 2017, ha impedito l'entrata in vigore dell'accordo tra Unione europea e Canada per lo scambio dei dati del codice di prenotazione (PNR). European Court of Justice, Opinion A1/15, 26 July 2017. A. Vidaschi, *Privacy and data protection versus national security in transnational flights: the EU-Canada PNR agreement*, in *International Data Privacy Law*, vol. 8, n. 2, 2018, pp. 124 ss.

dica dell'intelligenza artificiale – soprattutto se usata in funzione di tutela della sicurezza – in grado di rispettare gli “indicatori” prima esaminati e, quindi, assicurare il rispetto del principio di proporzionalità?

Ebbene, con riferimento al problema della mancanza di basi giuridiche chiare in materia, peraltro spesso rilevato dalle autorità garanti³⁴, la recente proposta di regolamento dell'Unione europea sull'intelligenza artificiale³⁵, presentata dalla Commissione europea, rappresenta uno *step* di rilievo. Infatti, la bozza di regolamento, nel vietare, in via generale, l'uso in luoghi pubblici di sistemi di riconoscimento facciale da parte delle autorità di polizia degli Stati membri, pone alcune limitatissime eccezioni. Stabilisce, cioè, che tali sistemi “intelligenti” di riconoscimento facciale possono essere usati solo per identificare persone che si sospetta stiano per porre in essere azioni di tipo terroristico. In questo modo, restringendo l'ambito di applicazione, la proposta fornisce – almeno indirettamente – una base giuridica per l'uso del riconoscimento facciale come tecnica *counter-terrorism*³⁶.

Relativamente ad altri usi dell'intelligenza artificiale a fini *counter-terrorism*, le basi giuridiche sembrano ancora assenti, se non a livello formale, perlomeno in un'ottica sostanziale. Si pensi al recente Regolamento (UE) 2021/784 sulla rimozione dei contenuti terroristici *online*. Sebbene siano disciplinate le modalità di rimozione, non vengono regolati in maniera stringente gli strumenti tecnologici da usare. La scelta di questi ultimi viene, ancora una volta, lasciata (quasi) totalmente ai privati. La base giuridica, perciò, seppure esistente, è assai vaga circa le applicazioni della tecnologia avanzata e, pertanto, non conforme al richiesto *standard* di precisione del *drafting*.

34 V. parere del Garante italiano del 25 marzo 2021, *cit.*

35 Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM/2021/206/final. V. C. Casonato, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, n. 3, 2021, pp. 1 ss.

36 Va tuttavia notato che lo European Data Protection Board e lo European Data Protection Supervisor, chiamati ad esprimere un parere congiunto sulla bozza di regolamento, hanno suggerito alla Commissione, nel giugno 2021, di eliminare totalmente la possibilità di utilizzo del riconoscimento facciale dalla bozza di regolamento, poiché si tratta di un sistema che agisce in modo sproporzionato sulla *privacy* dei cittadini. V. EDPB-GEPD, Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale), reperibile in https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_it.

Difficoltà circa la base giuridica e la sua chiarezza si pongono poi in materia di c.d. sorveglianza algoritmica, ossia gli algoritmi impiegati per incrociare e analizzare i metadati della comunicazione. A tal proposito, va ricordato che manca – dopo che la c.d. direttiva *data retention*³⁷ è stata invalidata dalla Corte di giustizia nel 2014³⁸ – una disciplina organica di livello eurolunitario. Di conseguenza, molto viene lasciato ai legislatori interni, i quali spesso adottano normative volutamente vaghe, come ha dimostrato l'esperienza francese.

Rispetto al tema del controllo *a priori* (c.d. *oversight* di autorità giudiziaria o amministrativa indipendente), qualcosa sembra essere in via di cambiamento. Invero, secondo la proposta di regolamento sull'intelligenza artificiale, i limitati casi in cui il riconoscimento facciale potrebbe essere utilizzato dovrebbero essere soggetti all'autorizzazione preventiva di un'autorità giudiziaria o perlomeno amministrativa indipendente³⁹. Invece, secondo il Regolamento (UE) 2021/784 (sulla rimozione dei contenuti terroristici *online*), l'eliminazione dei contenuti, inclusa quella con modalità automatiche, può avvenire su ordine di una "autorità competente", senza che ne sia precisata la natura. In termini più diretti, non viene imposto che questa sia un'autorità giudiziaria o perlomeno amministrativa indipendente⁴⁰, il che resta un elemento di criticità. E, inoltre, il Regolamento (UE) 2021/784 legittima un secondo tipo di rimozione, quella "proattiva" (si parla di c.d. misure specifiche) da parte del *provider* (e dei suoi algoritmi). Questa tipologia di eliminazione del contenuto, essendo rimessa *in toto* al privato, non vede alcun vaglio di matrice pubblicistica *a priori*.

Passando poi al controllo giurisdizionale *a posteriori*, tanto la proposta di regolamento sull'intelligenza artificiale (per la parte che concerne la sicurezza pubblica e, quindi, le tecniche di riconoscimento facciale) quanto la normativa sulla rimozione dei contenuti terroristici *online* intervengono

37 Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

38 Il riferimento è al caso *Digital Rights Ireland*, deciso della Corte di giustizia nel 2014 e citato *supra*.

39 Si veda l'art. 5, co. 3, del testo della proposta.

40 Le autorità competenti dovevano essere identificate dagli Stati membri entro il 7 giugno 2022 (con ampia discrezionalità degli Stati membri). Posto che, nel momento in cui si scrive (luglio 2022), non tutti gli Stati membri hanno ancora individuato le rispettive autorità, considerando le scelte fatte, non può non notarsi che la preferenza degli Stati è spesso stata espressa per organi di polizia o comunque con uno stretto legame con il potere esecutivo.

in questo senso. La proposta di regolamento, infatti, specifica che tutti gli utilizzi dell'intelligenza artificiale (inclusa l'unica fattispecie regolamentata impattante sulla sicurezza, ossia il riconoscimento facciale) devono poter essere sottoposti alla revisione di una autorità giurisdizionale. Pur essendo apprezzabile l'inserimento di questa disposizione, in quanto offre un segnale forte circa l'importanza della garanzia giurisdizionale, si devono rilevare alcune difficoltà pratiche, principalmente dovute al fatto che spesso, come si è visto, il processo algoritmico non è conoscibile interamente dall'operatore umano, e ciò potrebbe creare non poche difficoltà (se non effettivi impedimenti) all'organo giudicante. Ancor più sfidante per le operazioni di vaglio giurisdizionale risulta il Regolamento (UE) 2021/784, che parrebbe costituire, rispetto all'eventuale disciplina generale dell'*artificial intelligence*, una sorta di *lex specialis*. Esso si limita a specificare che i soggetti privati (*providers*) concretamente coinvolti nella rimozione sono tenuti a prevedere "meccanismi di reclamo"⁴¹, il che contribuisce alla delineazione di "strade alternative", aperte ad affidare il vaglio a soggetti carenti delle caratteristiche proprie delle autorità giudiziarie (autonomia, indipendenza, imparzialità, terzietà) e delle autorità amministrative indipendenti. Si tratta di organi "privati", spesso nominati dal *provider* e che dunque rispondono a quest'ultimo. Emblematico il caso, già menzionato, del Facebook Oversight Board.

6. Alcune osservazioni conclusive

Lo scenario, così come analizzato nel presente contributo, non può certo essere definito ottimale, visti i non trascurabili rischi posti dall'intelligenza artificiale, a cui si aggiungono gli innegabili *gaps*, tanto in termini di normazione quanto di garanzie.

Ciononostante, risulta altrettanto evidente che, in un mondo in crescente digitalizzazione, non si può fare a meno di impiegare lo strumento tecnologico, persino nel delicato settore della sicurezza. Di qui l'impellente necessità di una regolamentazione sistematica e ben strutturata. A tal proposito, va rilevato che vi sono stati significativi "passi in avanti", cioè non si è più al "punto zero". Per esempio, va rimarcato lo sforzo della Commissione per una regolamentazione eurounitaria sull'intelligenza artificiale, benché restino forti perplessità sullo spazio residuale lasciato al ricorso all'algoritmo nel campo della sicurezza pubblica. Inoltre, il regolamento

41 Art. 10, Reg. (UE) 2021/784.

sulla rimozione dei contenuti terroristici *online*, recentemente entrato in vigore, rappresenta un significativo sviluppo, soprattutto in considerazione dell'assenza, almeno in un primo momento, di fonti di matrice pubblicistica, al punto che l'identificazione e l'eventuale rimozione di contenuti terroristici *online* era totalmente lasciata a schemi di cooperazione informali tra i *big* della tecnologia. Meno positivo sembra il fatto che tale regolamento riservi spazio minimo (se non nullo) agli strumenti tecnici algoritmici da utilizzare per la rimozione.

Sono dunque ancora ampi i margini di miglioramento. Da un lato, sarebbe opportuno rafforzare il *corpus* normativo (per ora non inesistente ma sicuramente piuttosto scarso) orientato alla regolazione dell'intelligenza artificiale nel settore della sicurezza pubblica. In altre parole, i legislatori – soprattutto quello dell'Unione, al fine di assicurare uniformità e armonizzazione delle regole – dovrebbero adottare strumenti normativi specifici e dettagliati in materia di intelligenza artificiale finalizzata a garantire la sicurezza pubblica, così da arginare il proliferare della regolamentazione "privatistica". Dall'altro lato, a fronte dell'auspicio che la normativa di matrice pubblicistica si rafforzi, si deve tenere a mente che l'uso dell'intelligenza artificiale, poiché richiede competenze tecniche e risorse economiche, non può prescindere dalla cooperazione con il settore privato. In effetti, sarebbe impensabile sostenere che la *partnership* pubblico-privato in questo campo vada totalmente evitata.

L'esigenza di regolare l'intelligenza artificiale usata a scopi di sicurezza non può infatti ignorare la realtà, che vede le aziende private impegnate nell'ideazione degli algoritmi, grazie a competenze tecnologiche e risorse economiche che non sono nella disponibilità pubblica. Ciò posto, però, anche il ruolo dei privati dovrebbe essere oggetto di una attenta regolamentazione. In altre parole, senza ignorare le esigenze di mercato, la condivisione delle funzioni tra autorità pubbliche e attori privati del settore dovrebbe essere disciplinata da fonti di matrice pubblicistica, così da imporre agli operatori stringenti obblighi di rispetto del principio di proporzionalità e tra questi l'esclusione esplicita dell'impiego di quegli algoritmi il cui processo decisionale non risulti pienamente conoscibile.

Sullo sfondo di queste riflessioni, di portata anche "pratica", resta un tema teorico chiave: l'entrata in campo della tecnologia. Infatti, ancorché le competenti istituzioni adottassero un'adeguata regolamentazione dell'intelligenza artificiale, l'algoritmo è destinato a diventare un "attore principale", in quanto tecnicamente funzionale alla sicurezza; pertanto, entra, a pieno titolo, nel gioco dei bilanciamenti che coinvolgono diritti e libertà individuali. La conseguenza di questo "ingresso" dell'intelligenza

artificiale nel “perimetro” di azione delle libertà e dei diritti potrebbe significativamente trasformare la relazione sicurezza-diritti, un tempo concepita come binaria e ora aperta a inglobare un terzo fattore, appunto quello tecnologico. In definitiva, la tecnologia, nel configurare modi inediti tanto di godere dei diritti quanto di assicurare l’incolumità dello Stato e dei suoi cittadini, sembra quindi scardinare i paradigmi tradizionali.