INTELLIGENZA ARTIFICIALE, INFLUENZA SUL MERCATO POLITICO E REATI CONTRO LA PERSONALITÀ DELLO STATO. LA CRIMINALITÀ TERRORISTICA(*)

di Maurizio Romanelli

SOMMARIO: 1. Premessa. – 2. Intelligenza artificiale e terrorismo. – 3. Alcune precisazioni. – 4. Prospettive di impiego di A.I. da parte del terrorismo. – 5. Possibili conclusioni.

1. Premessa.

Il tema dei rapporti tra intelligenza artificiale e influenza sul mercato politico è particolarmente ampio; è quindi necessario operare alcune selezioni e procedere in prospettiva di sintesi e di semplificazione.

Atteso che viene chiesto di offrire anche dati di esperienza, preferisco concentrare l'attenzione sul mondo del terrorismo, prevalentemente internazionale, proponendo – in via di sintesi – alcune chiavi di lettura che nascono per l'appunto dall'esperienza, rinviando per analisi più sistematiche ad altri contributi[1].

L'esperienza sul mondo del terrorismo, e sul contrasto alle sue varie forme di manifestazione, può forse consentire di dare risposte ai due quesiti ormai quasi classici, intorno ai quali si muovono gli approfondimenti svolti in questa occasione di studio e di ricerca:

- l'Intelligenza Artificiale come strumento per la commissione di reati;

- l'Intelligenza Artificiale come (nuovo ed ulteriore) strumento di contrasto all'interno del sistema normativo dato.

Si tratta di due questioni che hanno rilevanza di carattere generale all'interno della macro-area dei rapporti tra intelligenza artificiale e sistema penale, ma che, ovviamente, assumono un rilievo del tutto peculiare rispetto ai fenomeni del terrorismo.

(*) Il presente contributo è già stato pubblicato sul quaderno II/2022 della *Rivista trimestrale della Scuola di perfezionamento per le forze di polizia*, curato dal Direttivo della Fondazione Vittorio Occorsio. Si ringraziano l'Editore e i curatori per averne autorizzato la pubblicazione su questa *Rivista*.

[1] Rinvio a C.O. ONORATI, *I.A., politica e reati contro la personalità dello Stato*, in *Sistema penale*, 13 giugno 2022, all'interno della raccolta degli atti del workshop della Fondazione Occorsio su *Intelligenza artificiale e giurisdizione penale*. Più in generale, su questioni classiche in tema di rapporti tra intelligenza artificiale e sistema penale, rinvio a F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto penale contemporaneo*, 29 settembre 2019.

2. Intelligenza artificiale e terrorismo.

Porto innanzitutto l'attenzione – all'interno dei limiti già indicati – sulla prima questione.

Vorrei cominciare offrendo in prima battuta dati di esperienza sulla realtà empirico-criminologica del terrorismo internazionale, quale si è manifestato a fare corso dalla data simbolo dell'11 settembre 2001 per circa un ventennio, passando dal tempo di *Al Qaida* all'affermazione di *Islamic State*, e poi nei diversi periodi di I.S.[2], sino alla sconfitta sul campo, ed all'attuale, quasi completa, scomparsa del c.d. terrorismo territoriale.

È ampiamente noto che si è trattato di un periodo terribile per una pluralità di Stati, europei ed extraeuropei, che hanno dovuto fare i conti – tutti – con la nuova realtà criminale e con le connesse esigenze di prevenzione/contrasto, attraverso il progressivo adeguamento della legislazione complessiva (non solo penale, ma anche processuale, ordinamentale, relativa alle agenzie di informazione, ecc.) e delle relative prassi di contrasto.

Do per acquisite, in questa sede, le conoscenze di base sull'evoluzione della nostra legislazione, a fare corso dall'immediato post torri gemelle, con il fondamentale d.l. n. 374 del 18 ottobre 2001, passando attraverso la riforma immediatamente successiva alla strage di Londra del 7 luglio 2005 (D.l. 144 del 27 luglio 2005) ed arrivando alla riforma successiva alla proclamazione di Islamic State ed alla ripresa degli attentati in Europa, soprattutto Parigi (D.l. n. 7 del 18 febbraio 2015).

Oggi ci troviamo di fronte ad una situazione in evoluzione, fluida, non facilmente decifrabile, sia per le caratteristiche evolutive del fenomeno criminale, che per il possibile "nuovo", determinato – appunto – tra le altre cose dall'evoluzione tecnologica.

Il "nuovo" è anche rappresentato dallo scoppio della pandemia da Covid-19, e dalla guerra di aggressione alle porte dell'Europa, *due ulteriori fatti inimmaginabili*, in aggiunta *all'inimmaginabile* rappresentato dall'attacco delle Torri Gemelle dell'11 settembre 2001.

Se è già molto complesso conoscere lo scenario e le linee evolutive del terrorismo c.d. islamico, la questione si complica ulteriormente se si porta l'attenzione sull'evoluzione del fenomeno del terrorismo su base suprematista, razzista, nazista, sulle sue reti, sui meccanismi di radicalizzazione e di passaggio all'azione, sui vari fronti e territori, soprattutto extraeuropei, ma con significative punte anche in Europa ed in Italia, come è purtroppo tristemente noto a partire dalla terribile strage di Utoya del 22 luglio 2011, fino alle gesta di Luca Traini del 3 gennaio 2018[3].

---

[2] Per una possibile individuazione di *periodi* all'interno dell'operatività dello Stato Islamico, e per la ricostruzione dei *relativi fenomeni criminali*, rinvio – per chi fosse interessato – a M. ROMANELLI, *Criminalità organizzata e terrorismo: la circolazione dei modelli criminali e degli strumenti di contrasto*, in *Sistema penale*, 20 dicembre 2019.

[3] Non mancano i precedenti significativi. Tra il giugno 2006 e l'aprile 2008 vi sono stati – tra Milano e provincia – oltre *una dozzina di attentati* a mezzo di molotov e di *pipe-bomb* in danno prevalentemente di luoghi di culto islamico, ma anche soltanto di luoghi legati al radicamento della comunità islamica in area milanese. Le indagini hanno consentito di chiarire che vi era un progetto puramente e semplicemente

In un quadro di questo tipo, le questioni relative all'impiego dell'intelligenza artificiale rappresentano prevalentemente ancora la formulazione di ipotesi, da una parte, e dall'altra la valutazione della minaccia in prospettiva di *capacity building* sul piano sovranazionale ed interno.

Senza pretese di completezza, proverò a delineare alcuni possibili impieghi di I.A. nel settore dei delitti contro la personalità dello Stato, e poi provo a ragionare sui relativi scenari.

La premessa necessaria è che il terrorismo c.d. islamico ha dimostrato ottima capacità di governo della tecnologia avanzata, soprattutto della rete internet e dei social media, utilizzandoli *con qualità crescenti* nel passaggio da *Al Qaida* ad *Islamic State*.

Questa "qualità" nella gestione delle tecnologie avanzate si è dimostrata essenziale rispetto ad alcune delle caratteristiche di fondo del terrorismo c.d. islamico e dei suoi fattori di forza: propaganda, arruolamento, addestramento ed autoaddestramento, radicalizzazione funzionale al passaggio all'azione, chiamata all'"egira"[4], rivendicazione di attentati e quindi ancora propaganda attraverso la rivendicazione, ecc.

Parallelamente l'evoluzione dei sistemi di intelligenza artificiale ha realizzato una maggiore accessibilità e facilità di uso degli stessi, e quindi anche una maggiore possibilità di forme di impiego.

Vi sono pertanto almeno due ragioni convergenti che impongono, o quanto meno giustificano, la domanda sul *"che cosa succede quando il terrorismo governa ed impiega l'A.I."*, oppure ancora sul *"è A.I. il futuro del terrorismo?"*.

3. Alcune precisazioni.

Svolgo innanzitutto una serie di precisazioni, assolutamente necessarie, sia pure in prospettiva di sintesi.

Prima precisazione.

---

antislamico. Il gruppo responsabile delle azioni si firmava *Fronte Cristiano Combattente*, ed aveva l'obiettivo di contrastare *con tutti i mezzi* la presenza dei musulmani in Italia. Il principale autore degli attacchi ricostruiti, e anche di altri in via di programmazione, era Roberto Sandalo, ex terrorista di Prima Linea, poi diventato fondamentale collaboratore di giustizia nel contrasto al terrorismo interno, e confluito infine su posizioni anti-islamiche tanto da operare come *Fronte Cristiano Combattente* per la lotta armata contro l'Islam ed i "*bastardi islamici*".

[4] La chiamata all'"egira" è l'*ordine* impartito da I.S. ad ogni "vero" musulmano di raggiungere il territorio dello Stato Islamico, abbandonando i territori della miscredenza: si tratta di un vero e proprio ordine, accompagnato dalla minaccia di pesanti conseguenze e sanzioni nel caso di inosservanza. È ovvio che la *hijra* è stata resa possibile, con imponenti fenomeni di emigrazione sia dall' Europa che da Paesi extraeuropei, nella misura *in cui vi fosse il territorio del Califfato*, e fin quando vi è stato. Numerose indagini svolte in Italia, attraverso la qualità dei nostri strumenti investigativi e l'esperienza delle nostre forze di Polizia, hanno dimostrato la centralità dell'ordine di raggiungere *Islamic State*, soprattutto nei primi mesi successivi alla proclamazione del Califfato da parte del "califfo" Abu Bakr Al-Baghdadi, e poi nei primi mesi del 2015.

Si tratta, come sopra detto, prevalentemente *di ipotesi di lavoro* per adeguare le capacità di risposta degli Stati e della comunità internazionale rispetto ad una valutazione di rischio.

Ma è necessario sempre accompagnare la formulazione di ipotesi con dati di conoscenza empirica effettiva, parametrati sulla realtà delle forme di manifestazione del terrorismo, e con l'impiego – sempre – di strumenti investigativi/preventivi efficaci, che consentano la migliore conoscenza del fenomeno e la maggiore tempestività possibile nella risposta.

È questo un aspetto importante, del quale discuto da tempo, soprattutto per segnalare quanto la positiva esperienza del nostro Paese nel contrasto a gravi forme di criminalità, quali il terrorismo interno e le mafie, abbia consentito di affrontare con tempestività ed efficacia la sfida portata dal terrorismo internazionale (addirittura già ben prima delle Torri gemelle)[5].

La "paura del nuovo possibile" deve sempre accompagnarsi all'attenzione sui dati di realtà, e ogni vera investigazione – anche la più tecnologicamente avanzata – deve e dovrà accompagnarsi sempre con la migliore possibile conoscenza dei fenomeni territoriali, delle persone in carne ed ossa, delle ragioni delle scelte radicali, delle motivazioni profonde (anche quando non sono profonde le motivazioni ci sono sempre in tema di terrorismo, e conoscerle è necessario in prospettiva di prevenzione ed anche, eventualmente, di "deradicalizzazione").

Ancora, sotto altro aspetto: la paura, ed ogni forma di narrazione allarmistica, in materie di così grande delicatezza, rappresentano anche fattori di *business* per una molteplicità di soggetti privati, individui e società, e quindi anche di tentativi di influenza/condizionamento sul mondo dei decisori pubblici.

La paura è strumento da maneggiare con cautela, e con consapevolezza di tutti i significati, anche puramente economici.

Seconda precisazione.

Si tratta di un discorso estremamente complesso, al quale faccio solo cenno, che rappresenta la chiave di volta di qualunque seria capacità di risposta ai fenomeni del terrorismo, sia giudiziaria che sul piano della prevenzione/sicurezza.

Il terrorismo attuale (in tutte le sue forme di manifestazione) è prevalentemente sovranazionale, e quindi soltanto la cultura reale della condivisione delle informazioni, della circolazione delle stesse, del confronto spontaneo tra gli attori del contrasto operanti nei diversi Stati, in un quadro di fiducia reciproca, può consentire risposte efficaci e tempestive.

Su questo tema molto è stato fatto negli ultimi anni, e l'Italia ha portato straordinari dati di esperienza e di metodo; molto però rimane da fare, ed è bene che sia sempre segnalata questa esigenza di fondo.

Terza precisazione.

---

[5] Per chi fosse interessato rinvio a M. ROMANELLI, *Riflessioni sul complessivo sistema di contrasto al terrorismo internazionale in Italia*, in *Diritto penale contemporaneo*, 14 giugno 2019.

Quale che sia il livello di aggressione a beni fondamentali, individuali e collettivi, portati dal terrorismo, nelle sue varie forme di manifestazione ed – in ipotesi – oggi "armato" di A.I., solo una risposta legale e rispettosa dei diritti è al tempo stesso efficace.

Come ho avuto già modo di evidenziare in altre occasioni, valorizzando le caratteristiche di fondo del contrasto al terrorismo nell'ambito del nostro sistema penale costituzionale, la forza dello Stato viene dalle regole: qualunque cessione di quote di regole giova solo alla causa del terrorismo, divenendo straordinario fattore di radicalizzazione ai fini dell'azione terroristica.

Non sono affermazioni vuote di contenuto, ma dati di esperienza univoci.

Anche ragionando su ipotesi di nuove forme di aggressione, e di nuove "sfide", il sistema di contrasto dovrà continuare ad offrire queste caratteristiche di fondo e rispettare queste regole fondamentali.

4. Prospettive di impiego di A.I. da parte del terrorismo.

Fatte queste premesse di metodo, è quindi del tutto corretto chiedersi quali sono le prospettive di impiego di A.I. da parte del terrorismo.

Semplificando, e seguendo le linee di approfondimento più aggiornate[6] a livello internazionale, le nuove minacce sono relative a tre macroaree:

A) cyber threats;
B) psysical threats;
C) political threats.

Alcuni cenni a ciascuna delle tre aree ed alcune riflessioni possibili, oltre che dati di esperienza.

A) Cyber threats

I *cyber attacks* sono una realtà, ormai da numerosi anni; sono modalità di aggressione con potenzialità offensive enormi e sono stati effettivamente usati da *Islamic State*.

[6] Si veda l'ampio rapporto "*Algorithms and terrorism: the malicious use of artificial intelligence for terrorist purposes*", redatto congiuntamente dal *Counter Terrorism* delle Nazioni Unite (UNCCT) e dal corrispondente centro di ricerca (UNICRI) nel 2021. Il rapporto appare apprezzabile anche perché *non* enfatizza il livello della minaccia, ma anzi muove dalla premessa dell'assenza di prove significative in ordine all'effettivo impiego di A.I. da parte di gruppi terroristici: "*From the outset, it is important to clarify that no clear evidence of the actual use of A.I. by terrorist organizations has been identified by date*". È però opportuno ricordare anche che il mondo del terrorismo internazionale si è mosso nel corso degli anni arrivando all'"inimmaginabile" – basta pensare alle stragi dell'11 settembre 2001 – e che quindi "*a failure of imagination can have deadly consequences*" (rapporto cit., p. 26). Del resto, la Commissione d'inchiesta degli Stati Uniti sull'11 settembre ha concluso i suoi lavori segnalando espressamente che è *un limite* non avere *capacità di immaginazione* quando ci si confronta con l'agire terroristico sovranazionale, invitando così le agenzie di controllo ad "*istituzionalizzare l'immaginazione*".

In tale settore, l'impiego dell'intelligenza artificiale appare tutto sommato semplice, e con capacità enorme di moltiplicazione dei risultati di offesa, soprattutto rispetto ad aggressioni abbastanza "basiche" quali quelle note come DoS o DDos.

Poco da dire – allo stato – sul piano del contrasto alla minaccia.

Si tratta di un classico problema di prevenzione/sicurezza, prima e più che di investigazione giudiziaria: le infrastrutture informatiche strategiche (economiche, militari, sistema di trasporti, salute, istruzione) devono avere livelli di protezione adeguati al livello della minaccia; la minaccia cresce e deve crescere la capacità di protezione.

Non molto dissimili le considerazioni di base in ordine ad altre note tipologie di aggressioni informatiche (*malware; ransomware; man-in-the-middle, ecc.*).

Non sembra che con riferimento a casi di questo tipo, destinati a crescere, siano possibili riflessioni ulteriori: si tratta di modalità di aggressione note, amplificate dalla capacità degli algoritmi di *machine learning*.

Certamente le cose si complicano enormemente con l'I.A. come aggressore e l'I.A. come difensore, o come aggressore di ritorno; ma dal punto di vista dei concetti di base, non mi sembra si vada oltre l'evidenziazione dell'esigenza di adeguata protezione/sicurezza.

Deve essere anche ricordato un altro aspetto, peraltro noto, e cioè che l'impatto dell'aggressione informatica può consistere non solo nella distruzione – totale/parziale, duratura/limitata nel tempo – di un sistema informatico, ma anche nella esfiltrazione di dati rilevanti, con successivi impieghi criminali dei dati stessi.

Ve ne sono stati numerosi esempi.

Senza entrare nei dettagli, un'aggressione informatica di questo tipo fu quella indirizzata nel 2015 contro una delle società leader a livello mondiale nella produzione e vendita di sofisticata tecnologia informatica, anche a Paesi stranieri, con sede a Milano.

All'esito dell'attacco informatico venne effettuata, sulla rete, la pubblicazione molto rilevante di dati sensibili, compreso il codice sorgente relativo al più raffinato sistema di presa di controllo di telefoni cellulari del tempo, che era venduto ad una pluralità di società che a loro volta offrivano la propria tecnologia al servizio di indagini, anche della Procura della Repubblica di Milano oltre che di altre Procure Distrettuali.

Il risultato immediato fu l'interruzione delle attività di intercettazione telematica ed ambientale che erano in corso in più procedimenti per fatti di terrorismo internazionale.

Il 2005, come è ampiamente noto, fu uno degli anni in cui più preoccupante era la progettualità terroristica verso i Paesi occidentali, Italia compresa, e la Procura di Milano dovette chiudere da un giorno all'altro attività di intercettazione molto utili, e cambiare radicalmente i programmi del proprio intervento, tra l'altro in un procedimento in cui il rischio di azione terroristica contro obiettivi situati all'interno dello Stato italiano era molto elevato.

Cambiò anche – di conseguenza – il rapporto tra prevenzione/sicurezza ed esigenze investigative, argomento di grandissima rilevanza nelle "vere" indagini di terrorismo, con la definitiva prevalenza dell'esigenza di prevenzione.

Molto in sintesi: se la tecnologia non offre più adeguato controllo degli indagati e delle loro attività (h. 24, come si dice in gergo), allora ci vuole un intervento immediato, o in termini giudiziari (se ve ne sono i presupposti) o in termini amministrativi (espulsione dal territorio dello Stato).

La materia è delicatissima, richiede esperienza e formazione, ma non è possibile trattarla qui adeguatamente.

B) Psysical threats

Per chi fosse interessato c'è ampia letteratura sul tema, soprattutto in lingua inglese, ma non vi sono troppe riflessioni da svolgere.

È ovvio che l'A.I. può rappresentare uno strumento per la moltiplicazione degli attacchi terroristici e per la maggiore efficacia degli stessi.

Gli esempi abitualmente fatti riguardano, prevalentemente, i due settori dell'impiego di droni, e dell'impiego di autovetture a guida autonoma (senza conducente) attraverso la presa di controllo del sistema di guida.

Vi sono in realtà ipotesi di lavoro ancora più drammatiche.

Ancora una volta si tratta di ipotesi possibili, rispetto all'impiego dei droni già in parte realizzate, che aggiungono qualcosa al livello della minaccia, che è e rimane alta a prescindere dall'impiego di sistemi di intelligenza artificiale (l'ipotesi non appare oggi molto lontana da altre fatte in passato in un crescendo di allarmi non sempre giustificati, come ad es. l'ipotesi della presa di possesso di centrali atomiche da parte di gruppi di terroristi, o di aerei militari, ecc.).

Deve essere aggiunto e valutato un dato di esperienza, noto agli attori del mondo del terrorismo.

Uno dei vantaggi tradizionalmente segnalati in relazione all'ipotesi dell'uso di *self-driving car* – grazie all'impiego di A.I. – è la non necessità del rischio di sacrificio della propria vita nella conduzione dell'attacco, o, in alternativa, la non necessità del rischio di "cadere prigionieri" del nemico che si vuole abbattere.

Si tratta di vantaggi possibili e correttamente enunciati, ma è bene ricordare che i meccanismi di radicalizzazione, particolarmente efficaci attraverso una grande capacità di propaganda, fanno riferimento all'azione individuale ed al sacrificio, fino all'attacco suicida, *come ad una delle massime realizzazioni dei doveri del combattente e quindi del "vero" musulmano.*

Già nel periodo di formazione di *Islamic State* come terrorismo territoriale, e poi durante il periodo di *Islamic State,* l'attacco suicida ha rappresentato un valore, non un rischio: valore fortemente rivendicato e propagandato attraverso una vera e propria procedura di comunicazione particolarmente efficace e che rappresentava un fortissimo collante.

Nella fase nota di maggiore potenza di *Islamic State* il sacrificio della vita è una forza, non un rischio da evitare[7].

---

[7] Il dato è abbastanza pacifico sia dal punto di vista empirico che nel quadro delle riflessioni sociologiche. Si veda, per chi è interessato all'approfondimento del tema, A. PLEBANI, *Jihadsmo globale. Strategie del terrore tra Oriente ed Occidente*, Giunti, 2016.

Questo non vuol dire che vi sia – o vi sarà – il rifiuto di mezzi aggressivi tecnologici che prescindano dal sacrificio della vita propria, ma solo per segnalare che la radicalizzazione è stata, ed è, centrale nell'affermarsi del *jihadismo* globale e passa attraverso il profondo coinvolgimento delle persone, in carne ed ossa, con il valore aggiunto del sacrificio della vita.

È certo però che uno spettacolare attacco realizzato attraverso la più avanzata tecnologia avrebbe quell'effetto di evidenza della propria forza, con connessa disseminazione della paura e del terrore, che rappresentano il mezzo dell'agire terroristico.

C) Political threats

L'argomento è oggetto di approfondimento in altra relazione e porto qui solo alcuni spunti utili al tema che tratto.

Il rischio di condizionamento della politica attraverso *deep fakes* è molto elevato sotto vari profili, e vi sono già stati esempi significativi in numerose parti del mondo, anche se forse l'impatto effettivo è stato minore rispetto alla valutazione di rischio effettuata negli anni scorsi. Solo a titolo di esempio di condizionamenti possibili, in svariate forme, pensiamo alle seguenti ipotesi: il condizionamento di elezioni attraverso la distruzione dell'immagine pubblica del candidato, o del partito o del movimento; la moltiplicazione dell'efficacia di discorsi d'odio, e quindi anche della radicalizzazione attraverso la rete, con l'ulteriore vantaggio di forme di anonimizzazione ancora più sicure.

Il contenuto audio-video falso o manipolato, realizzato attraverso sistemi di intelligenza artificiale, può avere efficacia devastante, sia per la qualità del falso che per la straordinaria capacità di disseminazione e per la velocità della stessa.

Nessuna controNarrazione, correzione, tentativo di eliminazione è in grado di sanare completamente l'effetto del falso.

Portando l'attenzione al mondo del terrorismo, emergono, nello specifico, due possibili riflessioni.

La propaganda online ha rappresentato uno dei più importanti fattori di successo del terrorismo c.d. islamico, così come la rete è il "luogo" d'eccellenza – non l'unico (pensiamo alle carceri) – per l'efficace funzionamento di meccanismi di radicalizzazione, e l'evoluzione tecnologica ha ovviamente contribuito in modo decisivo a questi successi.

In una prospettiva di studio particolare, prevalentemente psicoanalitica, si veda F. BENSLAMA, *Un furioso desiderio di sacrificio. Il supermusulmano*, Raffaello Cortina Editore, traduzione italiana del 2017. Il giorno prima degli attentati coordinati di Parigi, Fethi Benslama aveva pubblicato su Le Monde l'articolo "*Pour le désespérés, l'islamisme radical est un produit excitant*" (12 novembre 2015). Altro noto psicoanalista, Luigi Zoja, ha trovato una felice espressione sintetica: "*La sensazione di esistere non è consegnata dalla vita, ma dalla morte*" (L. ZOJA, *Nella mente di un terrorista. Conversazione con Omar Bellicini*, Einaudi, 2017, p. 73). Sulla "*morte cercata*", sul significato e valore, sono numerosi i contributi di Olivier Roy (più recente: O. ROY, *Le djihad et la mort*, Editions du Seuil, 2016; traduzione italiana: O. ROY, *Generazione Isis. Chi sono i giovani che scelgono il califfato e perché combattono l'Occidente*, Feltrinelli, 2017). Per alcune riflessioni su ulteriori dati di esperienza vedi anche M. ROMANELLI, *Brevi note sulla prevenzione della radicalizzazione jihadista*, in *Sistema penale*, 20 marzo 2020.

Basti pensare che ai tempi delle Torri gemelle, e durante l'organizzazione delle stragi in Europa, il sistema per la chiamata all'azione, per il consolidamento di scelte radicali, per la adesione all'idea del martirio viaggiava ancora prevalentemente su carta o sulle "famose" audiocassette contenenti le immagini dei martiri, gli inni al martirio, i canti di battaglia, che venivano trasportate fisicamente e clandestinamente, con assunzione di gravi rischi, nei luoghi dell'ascolto in comune e della radicalizzazione.

È pacifico quindi che l'intelligenza artificiale in questo settore *ha un presente ed un futuro.*

Una (possibile) riflessione.

La realtà, sapientemente montata ed illustrata, offre già di per se stessa grandi occasioni di contributo alla radicalizzazione, come l'esperienza delle investigazioni in materia ci ha dimostrato.

È sufficiente ricordare qui la "capacità" di radicalizzazione che hanno avuto da sempre le foto – pacificamente vere – delle varie forme di tortura che sono state utilizzate ad *Abu Ghraib* o le immagini degli "arancioni" di Guantanamo, che poi ritroveremo nelle tuniche fatte indossare agli ostaggi giustiziati dal nascente Stato Islamico.

Lo stesso effetto si è cercato di ottenere con le immagini terribili delle vittime dei bombardamenti, soprattutto bambini, accompagnate da frasi "classiche" di rivendicazione di attentati (*"il vostro sangue è forse diverso dal nostro?"*, o frasi di contenuto analogo[8]).

Questo non significa ovviamente che il *deep-fake* ha poco presente, o poco futuro, ma significa ancora una volta, e soltanto, fare i conti con i dati di realtà, e semmai ricordare con forza le regole di un sistema di contrasto al terrorismo che rispetti sempre i canoni di fondo del sistema penale costituzionale e del rispetto dei diritti.

5. Possibili conclusioni.

Per chiudere, con formule di sintesi:

– massima attenzione all'innovazione tecnologica, sempre, ed ancora di più oggi, atteso che l'A.I. è dato di realtà, e di uso ormai quasi comune;

– attenzione però sempre anche ai dati di conoscenza empirica dei fenomeni, alle ragioni delle scelte radicali, in una prospettiva di prevenzione/contrasto che individui le cause e che lavori su queste;

---

[8] Riproduco di seguito un passo della rivendicazione delle stragi dei treni di Madrid dell'11.3.2004, ma gli esempi offerti dall'esperienza sul campo delle indagini sono innumerevoli: "*... Sappiate che non avrete scampo e che Bush e la sua amministrazione vi porteranno solo distruzione. Noi vi uccideremo in ogni luogo ed in ogni tempo. Non ci sono differenze tra i civili ed i militari: le nostre vittime innocenti stanno morendo a migliaia in Afghanistan ed in Iraq. Il vostro sangue è più prezioso del nostro? Non avremo pietà con la vostra gente, vi uccideremo, porteremo la guerra nelle vostre case e voi non prenderete più sonno*". Non molti dissimili i concetti espressi da *Mohammad Sidique Khan,* cittadino inglese, nella sua rivendicazione delle stragi di Londra del Luglio 2005: "*... finchè voi non smetterete di bombardare, gassare, imprigionare e torturare il mio popolo, noi non termineremo questa lotta. Noi siamo in guerra ed io sono un soldato...*".

– ultimo: il rendere giustizia secondo le regole è il migliore antidoto al terrorismo ed alla visione radicale che lo sostiene; non è l'unico, e mai lo sarà, ma aiuta davvero.

Questi principi valgono, e devono valere, anche con riferimento alle nuove sfide.