UNIVERSITÀ DEGLI STUDI DI TRENTO
Facoltà di Giurisprudenza

# DIRITTO PENALE E MODERNITÀ

## Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali

*Atti del convegno*
*Trento, 2 e 3 ottobre 2015*

a cura di
ROBERTO WENIN
GABRIELE FORNASARI

2017

UNIVERSITÀ DEGLI STUDI DI TRENTO

Facoltà di Giurisprudenza

**QUADERNI DELLA FACOLTÀ DI GIURISPRUDENZA**

# 27

2017

Al fine di garantire la qualità scientifica della Collana di cui fa parte, il presente volume è stato valutato e approvato da un *Referee* esterno alla Facoltà a seguito di una procedura che ha garantito trasparenza di criteri valutativi, autonomia dei giudizi, anonimato reciproco del *Referee* nei confronti di Autori e Curatori.



ISBN 978-88-8443-726-6
ISSN 2284-2810



*Il presente volume è pubblicato anche in versione cartacea, grazie al contributo della Provincia autonoma di Trento, Servizio Istruzione e formazione del secondo grado, Università e ricerca, per i tipi di Editoriale Scientifica - Napoli (ISBN 978-88-9391-110-8).*

*Maggio 2017*

# DIRITTO PENALE E MODERNITÀ

## Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali

*Atti del convegno*
*Trento, 2 e 3 ottobre 2015*

a cura di
*Roberto Wenin*
*Gabriele Fornasari*

Università degli Studi di Trento 2017

# INDICE

Pag.

*Those who would give up essential Liberty,*
*to purchase a little temporary Safety,*
*deserve neither Liberty nor Safety.*
(Benjamin Franklin)

*The Security Council,* […] *condemning in the strongest terms all acts of terrorism irrespective of their motivation, whenever and by whomsoever committed, as one of the most serious threats to peace and security…*
(Resolution 1624 (2005))

# PREFAZIONE

*Roberto Wenin*

I gravi fatti di terrorismo avvenuti nel tempo intercorso tra la stesura della presentazione del convegno e la pubblicazione degli atti mi hanno indotto a riflettere.

In un suo recente contributo Massimo Donini si chiede: il clima politico, ermeneutico, giudiziario in Italia sarebbe differente se gli attentati si fossero verificati da noi? La stampa e l'opinione pubblica chiederebbero ai giudici e all'accademia da che parte stanno? La situazione nella quale si svolge il nostro dibattito non è ideale, ma semplicemente spesso astratta da una realtà che esiste in altre parti del mondo[1].

Per rendersene conto basti riflettere sulle naturali reazioni di fronte ai più "banali" episodi di microcriminalità che ci colpiscono personalmente e che sfociano istintivamente in richieste di maggiore sicurezza e rigore repressivo.

---

[1] M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione. Dal codice delle indagini preliminari a quello postdibattimentale*, in *Terrorismo internazionale. Politiche della sicurezza. Diritti fondamentali, Edizione speciale QG*, settembre 2016, 120 s.

Eppure ho ritenuto di mantenere quanto allora scritto per la presentazione dell'iniziativa, consapevole del monito sulla funzione del pensiero critico, sforzandomi di fare della censura il pregio rispetto ad una lucidità di pensiero, talora apparentemente asettica, alla quale come dottrina siamo chiamati in quello che è un delicato gioco di equilibri.

Il presente convegno nasce da un progetto di ricerca, che porta il medesimo titolo, il quale cerca di confrontarsi con le attuali sfide alle quali è chiamato il diritto penale, nella vertiginosa evoluzione tecnologica che caratterizza le società odierne. In tal senso un sentito ringraziamento va naturalmente alla Provincia autonoma di Trento e alla sensibilità da questa mostrata nel sostenere e favorire, tramite impegni concreti, la ricerca e il dibattito, non solo scientifico, rispetto a temi di profonda attualità e delicatezza che rappresentano le sfide con le quali è chiamata a confrontarsi la moderna società.

La rete globale nella sua dimensione virtuale rappresenta talora un mondo parallelo a quello reale, nel quale si infrangono i tradizionali limiti dimensionali, come ad oggi conosciuti. Tale luogo virtuale, delocalizzato e, al contempo, globalizzato, impone non solo di riconsiderare i problemi di disciplina, anche futura, in una prospettiva essenzialmente sovranazionale, ma di rivedere altresì il contenuto dogmatico di categorie fondamentali della teoria del reato e della procedura penale[2].

La rete globale ha creato dimensioni e spazi inaspettati, non solo per lo svolgimento di attività lecite, ma anche per rapporti di natura illecita o delinquenziale. Proprio per la sua dimensione globale e sovranazionale, la rete rappresenta il terreno di elezione per un altro fenomeno, quello del terrorismo internazionale di matrice fondamentalista, che pare sfuggire ai tratti caratteristici del diritto penale tradizionale, incentrato sul rapporto cittadino-Stato e abituato a confrontarsi su di un piano cul-

[2] Cfr. L. PICOTTI, *Internet e responsabilità penali*, in G. PASCUZZI, *Diritto e informatica. L'avvocato di fronte alle tecnologie digitali*, Milano, 2002, 115. Evidenzia la necessità che si estenda il sistema di garanzie costruito per il corpo fisico al corpo elettronico S. RODOTÀ, *Libertà personale. Vecchi e nuovi nemici*, in M. BOVERO (a cura di), *Quale libertà. Dizionario minimo contro i falsi liberali*, Roma-Bari, 2004, 50; solo così potrà essere ricostruita l'unità della persona ormai spezzata in una pluralità di «astrazioni di ciberspazio».

turale di natura essenzialmente omogenea[3]. Il disagio nell'affrontare tale fenomeno, così lontano dal tradizionale modello di criminalità organizzata, emerge già nelle difficoltà ad offrire una definizione unitaria di terrorismo; difficoltà che hanno spinto a privilegiare soluzioni di contrasto spesso settoriali, così dando adito alla critica di una valenza essenzialmente politica della scelta punitiva[4]. La rete per le sue caratteristiche – anonimato, rapidità e dinamicità dei flussi comunicativi, impatto mediatico – ha rappresentato lo strumento ideale per condotte di proselitismo, addestramento, reclutamento, reperimento di risorse e preparazione di attentati per fini terroristici. La dimensione sovranazionale del fenomeno criminoso e la natura "adimensionale" delle nuove tecnologie hanno reso sempre più pressante l'esigenza di una reazione a livello sovranazionale, innalzando organismi internazionali quali il Consiglio d'Europa, l'Unione europea, l'Onu a protagonisti indiscussi di una nuova fase di contrasto, con connessi problemi in termini di legittimazione democratica[5]. Lo sforzo verso una progressiva armonizzazione delle legislazioni nazionali, presupposto indefettibile per un'efficace strategia di contrasto, impone l'adozione di un metodo comparato che consenta di cogliere il reale contenuto delle modifiche normative, frutto spesso di frenesie interventiste legate all'emotività del momento[6].

---

[3] Cfr. A. GAMBERINI, *Profili di diritto penale sostanziale dell'azione di contrasto al terrorismo*, relazione tenuta in occasione dell'incontro di studio del C.S.M. sul tema «Terrorismo e Legislazione Penale», Roma 29-31 marzo 2004, reperibile sul sito *www.csm.it*.

[4] V. MASARONE, *Politica criminale e diritto penale nel contrasto al terrorismo internazionale. Tra normativa interna, europea ed internazionale*, Napoli, 2013, *passim*; cfr. R. BORSARI, *Diritto punitivo sovranazionale come sistema*, Padova, 2007, 80; J. FRIEDRICHS, *Defining the International Public Enemy: The Political Struggle behind the Legal Debate on International Terrorism*, in *Leiden Journal of International Law*, 2006, 69 ss.

[5] La critica si è rivolta per lo più alle risoluzioni emanate dalle Nazioni Unite, in particolare dal Consiglio di Sicurezza sulla base del capitolo VII della Carta: cfr. J. MACKE, *UN-Sicherheitsrat und Strafrecht. Legitimation und Grenzen einer internationalen Strafgesetzgebung*, Berlin, 2010, *passim*; F. RAUTENBERG, *Rechtsstaatswidriges Feindstrafrecht oder notwendige Maßnahmen zur Terrorismusbekämpfung? Zur Verfassungsmäßigkeit der §§ 89a, 89b und 91 StGB*, Baden-Baden, 2014, 53 ss.

[6] Sul punto sia consentito rinviare a R. WENIN, *L'armonizzazione delle legislazioni penali nazionali. Una riflessione comparata sulle strategie di contrasto muovendo dalle norme in materia di condotte con finalità di terrorismo*, in R. WENIN, G. FORNASARI,

Gli attuali interventi del legislatore italiano, per lo più attuati mediante decreto legge, riproducono troppo spesso consueti schemi, legati all'inasprimento sanzionatorio, volti più a rassicurare la popolazione che a rappresentare reali strumenti di contrasto rispetto a fenomeni che richiederebbero processi sinergici operanti su più piani e non meramente repressivi. Sono di tutta evidenza i limiti e l'insufficienza del diritto penale, soprattutto laddove lasciato solo.

La gravità della minaccia spinge sempre più l'intervento statuale, in un'ottica preventiva e punitiva, verso forme di anticipazione della tutela a condotte meramente prodromiche, spesso socialmente neutre, in cui rischia di assumere un valore esorbitante l'elemento volontaristico della direzione finalistica della condotta.

Tale frenesia interventista porta, nell'ottica panpenalistica, a rovesciare i tradizionali postulati dello Stato liberale, con perdita del carattere frammentario del diritto penale.

L'inevitabile ineffettività legata al ricorso esasperato allo strumento penale, che espone a pericolo la stessa coerenza sistemica, viene poi a sua volta rielaborata con il messaggio propagandistico della necessità di un maggiore rigore nel far rispettare la legge[7]. Al contempo l'emergenza terroristica instilla l'idea di una ineluttabile restrizione della libertà in favore della sicurezza[8], in ragione di un'asserita dicotomia fra sicurezza e libertà posta in termini di incompatibilità[9], sul presupposto che

---

E. FRONZA (a cura di), *La persecuzione dei crimini internazionali. Una riflessione sui diversi meccanismi di risposta. Atti del XLII Seminario internazionale di studi italo-tedeschi, Merano 14-15 novembre 2014. Die Verfolgung der internationalen Verbrechen. Eine Überlegung zu den Verschiedenen Reaktionsmechanismen. Akten des XLII. Internationalen Seminars deutsch-italienischer Studien, Meran 14.-15. November 2014*, Napoli, 2015, 193 ss.

[7] M. DONINI, *Sicurezza e diritto penale*, in *Cass. pen.*, 2008, 3558 s.

[8] Cfr. M. BOVERO, *Premessa. Il fantasma della libertà*, in ID. (a cura di), *op. cit.* in nota 2, IX, il quale fa riferimento ad una ideologia della sicurezza, concepita come *primum bonum* da salvaguardare in uno stato di eccezione planetario e permanente, e perciò invocata come criterio per giustificare ogni genere di limitazioni delle libertà fondamentali.

[9] Cfr. E. LO MONTE, *Gli interventi in tema di misure di prevenzione: il problema del congelamento di beni*, in A.A. DALIA (a cura di), *Le nuove norme di contrasto al terrorismo. Commento al Decreto-legge 27 luglio 2005, n. 144 convertito, con modifi-*

il probo cittadino non avrebbe nulla a temere e, anzi, una sua eventuale resistenza sarebbe quantomeno sospetta, secondo schemi tipici dei regimi totalitari[10].

Il pericolo diviene allora proprio quello di un'enfatizzazione e strumentalizzazione delle paure e insicurezze sociali al fine di veicolare limiti alle libertà, secondo il criterio dell'innesto all'apparenza innocuo e senza effetti collaterali[11].

L'arduo compito appare essere dunque quello di trovare un difficile equilibrio tra esigenze di tutela e la coerenza ai principi fondamentali di uno Stato liberale. Se da un lato è pur vero che non esiste una sconfinata prateria di internet dove tutto è permesso e niente è vietato[12], la retorica imperante sulla necessità di controlli rischia di sacrificare una quota eccessiva di libertà in nome di una sicurezza talora solo apparente[13]; libertà che costituisce il tratto caratteristico di una realtà acefala divenuta strumento principale di manifestazione del pensiero e luogo primario dello sviluppo economico e sociale.

Il convegno, strutturato su varie sessioni, di cui qui si pubblicano gli atti, mirava dunque a confrontarsi con i problemi testé evocati, soffermandosi su tematiche sia di diritto sostanziale sia di natura processuale.

---

*cazioni, nella Legge 31 luglio 2005, n. 155 ed integrato dal Decreto-legge 30 dicembre 2005, n. 272, convertito, con modificazioni, nella Legge 21 febbraio 2006, n. 49 e sintesi dei lavori parlamentari*, Milano, 2006, 441.

[10] Cfr. S. RODOTÀ, *op. cit.* in nota 2, 53 ss.

[11] G.M. FLICK, *Dei diritti e delle paure*, in S. MOCCIA (a cura), *I diritti fondamentali della persona alla prova dell'emergenza*, Napoli, 2009, 76.

[12] Tribunale di Milano, sentenza 24.02.2010 n. 1972, a firma del dott. Oscar Magi, 95; reperibile sul sito *www.penalecontemporaneo.it*. Sentenza pronunciata nel noto caso Google/Vivi Down nella quale ci si interrogava sugli obblighi gravanti in capo agli ISP.

[13] Così F. CHIUSI in occasione del *Festival Vicino/Lontano Digital 2015. Internet, terrorismo e democrazia: l'arte sottile del controllo pervasivo*, tenutosi a Udine dal 7 al 10 maggio 2015.

# INTRODUZIONE

*Giuseppe Nesi*

Benché il fenomeno abbia radici antiche, è un fatto che dall'inizio del nuovo millennio e cioè da più di quindici anni – un tempo lunghissimo nell'era di tumultuoso sviluppo tecnologico e delle comunicazioni che stiamo vivendo – le istituzioni internazionali, i governanti di tutti i Paesi e l'opinione pubblica mondiale hanno dovuto fare quotidianamente i conti con l'esplosione a livello globale del terrorismo internazionale.

Fino alla fine degli anni '90 il terrorismo era visto per lo più in un'ottica nazionale, in cui ciascuno Stato approntava gli strumenti che riteneva maggiormente idonei ad affrontare il fenomeno. Non mancavano ovviamente tentativi di regolamentarlo a livello internazionale, per lo più scaturenti da eventi specifici che hanno tuttavia favorito l'adozione di numerose convenzioni internazionali di tipo settoriale che per lungo tempo sono state ratificate da un numero ridotto di Stati.

Tutto è cambiato tra la fine del secolo scorso e l'inizio di quello in cui viviamo. In primo luogo, il Consiglio di sicurezza dell'ONU adottò una serie di risoluzioni che determinarono un mutamento radicale nelle politiche di contrasto al terrorismo con ripercussioni sugli Stati e sugli individui. Il Consiglio di sicurezza, andando secondo alcuni anche al di là delle proprie competenze, ha posto una serie di obblighi vincolanti nella lotta al terrorismo che incidevano profondamente sugli assetti costituzionali degli Stati membri; agli Stati nel loro complesso è stato anche richiesto d'indicare alle Nazioni Unite, o meglio al Consiglio di sicurezza, individui e entità sospettati di porre in essere atti di terrorismo e di sostenere e finanziare il terrorismo internazionale. Individui e entità che sono stati sottoposti dal Consiglio di sicurezza e dai suoi organi sussidiari a rigide sanzioni, anche di tipo economico, mediante decisioni contro le quali nessun tipo di ricorso era ammesso, con evidente violazione di alcuni diritti fondamentali garantiti dalle Costitu-

zioni e dalle leggi degli Stati membri. Subito dopo gli attentati del 2001 il Consiglio di sicurezza si spinse fino a imporre agli Stati di aderire alle convenzioni settoriali in materia e di adottare leggi che criminalizzassero il fenomeno e combattessero gli autori, i finanziatori e i sostenitori del terrorismo internazionale, denunciando così alcune delle lacune che hanno facilitato l'esplodere del fenomeno.

Inutile dire che gli Stati più autoritari (o meno liberali) approfittarono di questi momenti e dello stato di emergenza che ne risultò per adottare, a livello interno, una serie di misure fortemente repressive dei diritti fondamentali. E d'altra parte è significativo che, a parte i generici richiami alla tutela dei diritti fondamentali in una serie di risoluzioni del Consiglio di sicurezza, richiami a volte accompagnati da più o meno adombrate riserve, soltanto nel 2004 il Consiglio di sicurezza adottò una risoluzione in cui affermò con forza l'obbligo di tutelare i diritti fondamentali nella lotta al terrorismo internazionale. E tale affermazione – per quanto paradossale possa apparire – fu fatta più che altro allo scopo di denunciare le gravi violazioni di cui alcuni Stati occidentali si resero responsabili dopo l'occupazione dell'Iraq. Basti pensare alle immagini delle torture nelle carceri di Abu Ghraib.

Quanto avvenuto successivamente è ben noto, con i numerosi ricorsi presentati di fronte alle giurisdizioni nazionali e ai tribunali internazionali competenti in materia di diritti fondamentali dalle presunte vittime di ripetute e ingiustificate violazioni di tali diritti e le posizioni, spesso imbarazzate, assunte dai giudici nonché la denuncia di tali pratiche. Ricorsi e denunce che hanno messo in discussione in sede giurisdizionale l'autorevolezza e il ruolo del Consiglio di sicurezza e più in generale dell'ONU. E ciò è avvenuto anche in Paesi tradizionalmente sostenitori delle istituzioni internazionali o nel quadro di organizzazioni regionali.

Dall'altro lato, le organizzazioni terroristiche adottavano tecniche sempre più sofisticate dal punto di vista della comunicazione, del reclutamento e dell'impatto delle loro azioni sull'opinione pubblica, in operazioni che, a loro avviso, non potevano che concretizzarsi in una "guerra" contro gli Stati nei cui territori le operazioni terroristiche venivano realizzate. Perpetuare uno stato di "permanente" emergenza le-

gittimava e rafforzava, dal punto di vista delle organizzazioni terroristiche, la loro presenza e le loro azioni sullo scenario internazionale.

In tale contesto, un convegno come quello organizzato qui a Trento dai colleghi penalisti non può che costituire un'eccellente occasione di confronto e di approfondimento su molte delle questioni connesse alla tutela dei diritti umani nella lotta al terrorismo che si sono poste nel corso degli ultimi quindici anni e di quelle che si presenteranno negli anni a venire dal momento che il fenomeno del terrorismo internazionale, riemerso in tutta la sua gravità in tempi recenti, non sembra destinato a cessare nei prossimi anni.

La comunità internazionale, e ciascuno Stato che ne fa parte e che al terrorismo internazionale intende opporsi, deve utilizzare al meglio i mezzi a propria disposizione nonché trovare nuove forme di contrasto facendo ricorso – nel rispetto dei diritti fondamentali sul piano interno e internazionale – a tutti gli strumenti, anche quelli più moderni e sofisticati, per prevenire le sue azioni e combatterlo con lo scopo di mantenere e rafforzare lo stato di diritto e di tutelare coloro che del terrorismo internazionale sono per definizione le vittime, e cioè gli individui. Guai a cedere alla tentazione, a volte ahimè assai efficace, di ignorare il rispetto di tali diritti, anche nella lotta al terrorismo.

# PRIMA SESSIONE

# LE NUOVE EMERGENZE TERRORISTICHE: IL DIFFICILE RAPPORTO TRA ESIGENZE DI TUTELA E GARANZIE INDIVIDUALI

*Antonio Cavaliere*

SOMMARIO: *1. I beni giuridici tutelati dall'intervento penale in materia di terrorismo. 2. I principi relativi al bilanciamento dei beni secondo la Costituzione e la loro validità generale. 3. Le tendenze verso uno svuotamento 'realistico' dei principi costituzionali. 4. Un terreno nevralgico: la punibilità di accordi ed atti preparatori. 5. Associazione terroristica e finalità di terrorismo. 6. Singole ipotesi di punibilità di atti preparatori non 'associati'. 7. Cenni intorno alle misure di prevenzione antiterrorismo. 8. Rilievi conclusivi. Il* trend *internazionale ed europeo e le alternative proponibili dalla cultura penalistica.*

## *1. I beni giuridici tutelati dall'intervento penale in materia di terrorismo*

Dal punto di vista penalistico, i fatti di terrorismo – al di là delle numerose, diverse definizioni sociologiche o di diritto internazionale del fenomeno[1] – si connotano per la gravità dei danni e dei concreti pericoli che essi comportano per la vita e l'incolumità di molte persone, prima che per il patrimonio pubblico e/o privato. È anzitutto la dram-

[1] Secondo un'icastica osservazione di Helmut Schmidt, «ciascuno può definire ciascuno terrorista»; cfr. in proposito M. KRIELE, *Völkerrecht im Werden*, in *ZRP*, 2011, 184. Sulle gravi difficoltà di una definizione di terrorismo, v., da una prospettiva sociologica, v. per tutti, D. TOSINI, *Terrorismo e antiterrorismo nel XXI secolo*, Roma-Bari, 2007, 3 ss.; da un punto di vista criminologico, ad es. H.-J. ALBRECHT, *Terrorismus und Strafrecht*, in R. GRIESBAUM, R. HANNICH, K.H. SCHNARR (hrsg. von), *Strafrecht und Justizbewährung. Festschrift für Kay Nehm zum 65. Geburtstag*, Berlin, 2006, 17 ss.; sul problema definitorio in diritto internazionale, cfr. spec. T. WEIGEND, *The Universal Terrorist. The International Community Grappling with a Definition*, in *JICJ* 4 (2006) (consultabile *online* su *jicj.oxfordjournals.org*), 914 ss., secondo cui – *ivi*, 926 – non può ancora parlarsi di una definizione internazionalmente condivisa di terrorismo.

matica lesività di quei fatti – si pensi, ad esempio, alla strage di Piazza Fontana o a quella dell'11 settembre 2001 – a rendere il fenomeno criminale 'terroristico', nel senso di idoneo – prima che soggettivamente diretto – a terrorizzare la collettività.

Una tale premessa, apparentemente elementare, risulta necessaria per una corretta individuazione degli elementi da bilanciare quando è in gioco un intervento penale. Si tratta, infatti, di un intervento lesivo di libertà e dignità di una persona "in carne ed ossa", che nel nostro ordinamento, per il principio di offensività, si giustifica solo in presenza del danno o del pericolo per beni giuridici di rango costituzionale proporzionato; beni che, in virtù del principio di determinatezza (art. 25 co. 2 Cost.), devono essere precisamente definiti e la cui offesa dev'essere empiricamente verificabile.

Non possono, quindi, evocarsi oggettività giuridiche vaghe, affette da gigantismo e dall'inafferrabilità dell'offesa, quali l'ordine pubblico – interno o, addirittura, mondiale –, la personalità dello Stato, la 'sicurezza'[2]. Quest'ultima, in particolare, è un'entità che, nella sua onnicom-

[2] In particolare, per una critica del riferimento al bene 'sicurezza', cfr. F. PALAZZO, *Contrasto al terrorismo, diritto penale del nemico e principi fondamentali*, in *Quest. giust.*, 2006, 673: «La sicurezza come criterio di selezione di tipi criminosi si rivela un po' simile al valore dell'"obbedienza come tale" di antica memoria […] Non solo qualunque fatto violento si pone naturalmente in contrasto con la sicurezza, ma qualunque fatto anche lontanamente prodromico a quello è capace di attentare alla sicurezza. Se a tutto ciò si aggiunge che il diritto alla sicurezza viene elevato a presupposto di tutti gli altri diritti fondamentali, così da attribuire ad esso una sorta di primato, ne risulta profondamente alterato il giudizio di bilanciamento con i diritti di libertà. In sostanza, il diritto alla sicurezza diventa potenzialmente *onnivoro* rispetto a tutti gli altri diritti fondamentali […]. L'esito finale di questa operazione mistificatoria è lo scardinamento dell'intero sistema costituzionale dei diritti fondamentali […]». Contro l'esaltazione di un onnivoro 'diritto alla sicurezza', in favore della sicurezza dei diritti di tutti i consociati, limpidamente A. BARATTA, *Diritto alla sicurezza o sicurezza dei diritti?*, in S. ANASTASIA, M. PALMA (a cura di), AA.VV., *La bilancia e la misura. Giustizia, sicurezza, riforme*, Milano, 2001, 19 ss.; cfr. pure M. PAVARINI, *Degrado, paure e insicurezza nello spazio urbano*, in M. DONINI, M. PAVARINI (a cura di), AA.VV., *Sicurezza e diritto penale*, Bologna, 2011, 55-56. Sia consentito rinviare inoltre al nostro *Può la 'sicurezza' costituire un bene giuridico o una funzione del diritto penale?*, in W. HASSEMER, E. KEMPF, S. MOCCIA (a cura di), *In dubio pro libertate. Festschrift für Klaus Volk zum 65. Geburtstag*, München, 2009, 111 ss. e in *Crit. dir.*, n. 1-4/2009, 43 ss.

prensività, comprende beni di rango molto diverso ed anche mere sensazioni individuali; assumendo quale bene giuridico la 'sicurezza' si può arrivare a punire, ad esempio, mendicanti e lavavetri, o magari, per quel che concerne la prevenzione del terrorismo, donne islamiche che circolino a volto coperto o immigrati e profughi sospettati di essere genericamente 'legati' ad ambienti fondamentalisti.

A mio avviso, la strage dell'11 settembre e quelle di Londra, Madrid, Parigi non hanno offeso, né posto seriamente in pericolo, in modo concreto ed attuale, gli Stati coinvolti, né l'ordine pubblico o la personalità dello Stato o la 'sicurezza'[3]; piuttosto, essi hanno strappato la vita a migliaia di persone. Sono le loro vite i beni offesi; sono loro le vittime di quelle stragi, e non lo Stato, la sicurezza o l'ordine mondiale. Un ordine mondiale che, oltretutto, quale asserito oggetto di tutela appare problematico, perché presenta anche qualche tratto di iniquità e di oppressione; ma sul punto e sul dilemma delle cause del terrorismo e dei relativi rimedi si tornerà più avanti.

Naturalmente, dalla corretta definizione dei beni in gioco discendono, in diritto penale, diverse conseguenze. Una di esse riguarda, com'è noto, la corretta individuazione del grado di anticipazione della tutela e, quindi, la corretta impostazione del problema relativo alla legittimità di tale anticipazione.

## *2. I principi relativi al bilanciamento dei beni secondo la Costituzione e la loro validità generale*

Anche quando, come in materia di terrorismo, si tratta di fronteggiare fatti offensivi di beni fondamentali di molte persone, la nostra Costituzione, inserita in una cornice europea di tutela dei diritti dell'uomo, sancisce alcuni principi penalistici inviolabili, che tutti conosciamo e che costituiscono i criteri vincolanti del bilanciamento tra i beni giuridici dei consociati: legalità di reati e pene, offensività, personalità della responsabilità penale, divieto di trattamenti contrari al senso di umanità

[3] Similmente, segnala la difficoltà di simili giudizi di 'macrolesività', in riferimento alla definizione di terrorismo contenuta nella decisione-quadro europea del 2002, T. WEIGEND, *The Universal Terrorist*, cit., 927.

e tensione verso la rieducazione – da intendersi quale reinserimento sociale –, divieto assoluto della pena di morte. A tali principi vanno aggiunti quelli processuali, quali il diritto di difesa, il diritto al giudice naturale precostituito per legge, la presunzione di innocenza e il diritto ad un giusto processo[4].

Nessuno di tali principi può soccombere in un ipotetico bilanciamento con esigenze 'generalpreventive', o di 'ordine pubblico' e 'sicurezza' o di tutela di diritti fondamentali delle vittime[5]. Al contrario, ciascuno di quei principi fa parte dell'ordine costituzionale, quale insieme di criteri, sanciti dalla Legge fondamentale, del bilanciamento tra interessi individuali e collettivi; criteri del bilanciamento che non sono a loro volta bilanciabili[6]. Ciascuno di tali criteri mira a tutelare i diritti fondamentali di tutte le persone coinvolte in un conflitto individuale/sociale.

Inoltre, tutti quei principi valgono per ogni essere umano. La Costituzione non prevede, anzi, non tollera discriminazioni sul punto: ad

[4] Una tale premessa generale è limpidamente delineata da S. MOCCIA, *La perenne emergenza. Tendenze autoritarie nel sistema penale*, 2ª ed., Napoli, 1997, 14 ss.

[5] Emblematiche di una visione fuorviante del bilanciamento tra principi ed 'emergenze' appaiono le considerazioni di F. MANTOVANI, *Diritto penale*, *Parte generale*, 5ª ed., Padova, 2007, 207 ss.; l'illustre Autore sostiene – nonostante il rango costituzionale del principio di offensività – la legittimità di reati "senza offesa", motivandola con «l'irrinunciabilità di *deroghe* [al principio di offensività] per la prevenzione delle lesioni a beni primari, da contenersi nei limiti della necessità ed eccezionalità» (p. 210); anche il «diritto penale preventivo, con anticipazioni dell'incriminazione a fasi preoffensive, trova la sua legittimazione in base al principio costituzionale della prevenzione della lesione o messa in pericolo del bene», *ivi*, 220. La Costituzione conterrebbe, dunque, il principio di offensività, secondo cui non si può punire in assenza di un'offesa, e quello "di prevenzione" – il cui fondamento è tutto da individuare –, secondo cui si può punire in assenza di un'offesa.

[6] Sull'illegittimità di una relativizzazione dei principi penalistici, con particolare riferimento al principio di personalità della responsabilità penale di cui all'art. 27 co. 1 Cost., cfr. Corte cost., sent. 1 agosto 2007, n. 322, punto 2.3 del *considerato in diritto*, in *www.cortecostituzionale.it*: «Il principio di colpevolezza non può essere "sacrificato" dal legislatore ordinario in nome di una più efficace tutela penale di altri valori, ancorché essi pure di rango costituzionale. I principi fondamentali di garanzia in materia penale, difatti, in tanto si connotano come tali, in quanto "resistono" ad ogni sollecitazione di segno inverso».

esempio, per quanto siano orribili ed esecrabili i meri propositi e gli atteggiamenti interiori, essi non legittimano mai l'intervento penale, in rapporto a nessuno, neppure al più fanatico ed invasato dei fondamentalisti sedicenti islamici. Ancora, le pene devono tendere al reinserimento sociale, persino in rapporto agli autori dei più atroci delitti[7]. Tutti sappiamo che esistono ex terroristi che hanno abbandonato la lotta armata e conducono una nuova vita; scontata la pena, che dev'essere sempre strutturata come offerta di recupero sociale, essi hanno il diritto di rientrare nella società, magari mantenendo le proprie intime convinzioni – giacché una rieducazione rispettosa della persona non può violarne l'autonomia morale –, purché non aggrediscano beni giuridici altrui. Per quel che concerne l'esecuzione della pena – ma considerazioni analoghe valgono, *mutatis mutandis*, per l'esecuzione di qualsiasi misura cautelare o di detenzione sedicente 'amministrativa' –, nessun reato giustifica un'esecuzione della pena inumana o incentrata sulla mera neutralizzazione, anziché sull'offerta di reinserimento sociale: in Italia non possono esistere Guantanamo o gli orrori di Abu Ghraib. E nessun imputato o indagato può essere costretto ad accusare sé o altri o sottoposto a tortura.

Ecco perché un 'diritto penale del nemico', che neghi ad alcuni individui, definiti "non persone", i diritti fondamentali e le garanzie costituzionali del sistema penale, contrasta con la garanzia di quei diritti ad

[7] Per un non condivisibile 'affievolimento' del finalismo rieducativo di cui all'art. 27 co. 3 Cost. – *rectius* per una deroga allo stesso – in rapporto a gravi forme di criminalità, cfr. G. MARINUCCI, E. DOLCINI, *Manuale di diritto penale*, *Parte generale*, Milano, 2004, 13: «La rieducazione deve inoltre cedere il passo alla neutralizzazione del condannato, qualora questi non sia suscettibile nè di essere reinserito nella società attraverso l'esecuzione della pena, né appaia sensibile ai suoi effetti di intimidazione-ammonimento. Emblematico il caso di molti esponenti di spicco della criminalità organizzata, dalla mafia alle organizzazioni terroristiche»; per una valorizzazione della neutralizzazione in relazione al terrorismo v. pure F. VIGANÒ, *Terrorismo, guerra e sistema penale*, in *Riv. it. dir. proc. pen.*, 2006, 694. Contro siffatte deroghe al principio rieducativo recentemente F. MUÑOZ CONDE, *De la tolerancia cero al Derecho penal del enemigo*, Managua, 2005, 72; per un'autorevole critica verso il perseguimento di istanze di 'sicurezza' *sub specie* neutralizzazione, in contrasto con i principi costituzionali del diritto penale, cfr. W. HASSEMER, *Sicurezza mediante il diritto penale* (2006), in *Crit. dir.*, n. 1-2/2008, 35-36.

ogni persona; contrasta con l'art. 3 Cost. e con tutti i principi menzionati. Jakobs e qualche suo seguace ritengono legittimo, nei confronti dei nemici, in particolare dei terroristi, in quanto "non persone", punire mere manifestazioni soggettive di pericolosità, neutralizzarli internandoli a tempo indeterminato e torturarli[8]. Anche nell'ordinamento tedesco, al cui interno è stata elaborata quell'aberrante costruzione teorica, essa contrasta con lo spirito della Costituzione, a partire dall'art. 1 *Grundgesetz*, che, nell'affermare l'inviolabilità della dignità umana, non tollera l'esclusione di "non persone"; e tale solenne affermazione scaturisce proprio dal ripudio dell'esperienza nazionalsocialista dell'esclusione, fino all'annientamento, di alcuni esseri umani dai diritti fondamentali.

### *3. Le tendenze verso uno svuotamento 'realistico' dei principi costituzionali*

Una parte della dottrina italiana, pur respingendo la teorizzazione di Jakobs, ha tentato in vario modo di ridimensionare la cogenza o la portata dei principi costituzionali citati, a fronte di fenomeni criminali particolarmente gravi come terrorismo e criminalità organizzata di tipo mafioso, ma non solo; si pensi a forme particolarmente gravi di delinquenza sessuale.

La comune premessa pare essere un preteso 'realismo' che rifugga da mere utopie[9]. Il sistema penale prevede già la punibilità del mero accordo e di atti preparatori, nonché una polifunzionalità della pena nella quale prevalgono talora componenti repressivo-deterrenti e neutralizzanti: con conseguenti sanzioni sproporzionate al reato commesso,

[8] Per una critica del diritto penale del nemico, sia consentito rinviare al nostro *Diritto penale "del nemico" e "di lotta": due insostenibili legittimazioni per una differenziazione, secondo tipi d'autore, della vigenza dei principi costituzionali*, in *Crit. dir.*, n. 4/2006, 295 ss. e in AA.VV., *Delitto politico e diritto penale del nemico*, a cura di A. GAMBERINI, R. ORLANDI, Bologna, 2007, 265 ss., con ult. rif. bibl.

[9] Un tale orientamento "realistico" è autorevolmente sostenuto, come si è accennato in rapporto al principio di offensività, da F. MANTOVANI, *Diritto penale*, *Parte generale*, cit., 207 ss.

forme di carcere duro in funzione di coazione a collaborare e simmetriche esclusioni dai benefici penitenziari orientati alla rieducazione. In presenza di un'emergenza terroristica o mafiosa o di altre 'perenni emergenze', l'allarme sociale manipolato dal circuito politico-mediatico rischia di esasperare tali tratti autoritari del sistema penale: si ritiene, dunque, che si debba riconoscerli e 'governarli'.

In effetti, anche la teorizzazione di Jakobs si fonda sulla descrizione di una realtà legislativa e finisce – in modo a volte ambiguo, a volte scoperto – per legittimarla, fondandola sulla distinzione tra diritto penale del cittadino e del nemico. Egli afferma di voler separare quest'ultimo dal diritto penale del cittadino, per salvaguardare, solo per quest'ultimo, le garanzie costituzionali[10]. Così, nella dottrina italiana si riconosce che esistono norme di legge in tensione con i principi costituzionali, e ci si preoccupa di 'razionalizzarle', fornendo loro legittimazione. Magari, parlando di diritto penale 'di lotta' anziché del nemico[11]. Certo, non si arriva all'eccesso di proporre pene indeterminate, esecuzione degradante e tortura. Ma ciò che si finisce per legittimare è un orientamento politico-criminale volto alla neutralizzazione della pericolosità, di ascendenza positivista, strutturalmente del tutto analogo a quello proposto da Jakobs: orientamento che, naturalmente, ha anche una funzione simbolica di stabilizzazione dei consensi dei 'cittadini', ma in cui tale rassicurazione collettiva si regge sull'ideologia della neutralizzazione della pericolosità.

Tale ideologia si riflette, sul piano della condotta punibile, nell'eccezionale anticipazione della tutela ad atti preparatori, al mero accordo ed alla mera manifestazione di pensiero; sotto il profilo delle sanzioni, in pene sproporzionate al fatto commesso ed orientate alla pericolosità

[10] Cfr. G. JAKOBS, *Terroristen als Personen im Recht?*, in *ZStW*, 2005, 850-851; ID., *Staatliche Strafe: Bedeutung und Zweck*, Padernborn, 2004, 45; nel senso della necessità di una precisa demarcazione, cfr. peraltro già G. JAKOBS, *Kriminalisierung im Vorfeld einer Rechtsgutsverletzung*, in *ZStW*, 1985, 784.

[11] M. DONINI, *Il diritto penale di fronte al "nemico"*, in *Cass. pen.*, 2006, 736 ss.; F. MANTOVANI, *Il diritto penale del nemico, il diritto penale dell'amico, il nemico del diritto penale e l'amico del diritto penale*, cit., 478 ss.; criticamente sul punto M. PAVARINI, *La giustizia penale ostile*, in *Studi sulla questione criminale*, 2007, 14 ss.; v. pure il nostro *Diritto penale "del nemico" e "di lotta"*, cit., 280 ss.

soggettiva; sul versante processuale, in un "doppio binario", che riguarda, in particolare, le misure cautelari – strumentalizzate in chiave di prevenzione speciale – e l'esecuzione penale, in riferimento al regime differenziato di cui agli artt. 4 *bis* e 41 *bis* co. 2 ord. penit., che prevede l'esclusione di misure alternative e forme di carcere duro – una tortura *soft* – volte a costringere alla collaborazione processuale.

Si possono individuare tre percorsi volti alla legittimazione teorica di quel diritto penale 'eccezionale' orientato alla neutralizzazione della pericolosità.

Un primo percorso è quello seguito da chi propone di introdurre nella Costituzione delle clausole espresse di deroga a determinati principi costituzionali in tempo d'emergenza[12]. Ora, a parte i rischi insiti nell'individuazione dei principi ai quali derogare – quasi che vi fossero in materia penale principi costituzionali 'secondari' e, come tali, rinunciabili – e dei presupposti del verificarsi di un simile "stato di eccezione", ciò equivale ad una pericolosissima sospensione dei principi costituzionali, che, al di là delle intenzioni di chi la propone, ha un sapore manifestamente autoritario.

Un secondo percorso argomentativo, non meno inquietante, propone di ravvisare nell'emergenza un limite implicito ai principi costituziona-

[12] Per un'articolata proposta di prevedere una clausola espressa di 'emergenza' v. spec. R. BARTOLI, *Lotta al terrorismo internazionale. Tra diritto penale del nemico,* jus in bello *del criminale e annientamento del nemico assoluto*, Torino, 2008, 187 ss., secondo cui ciò non comporterebbe rischi di eversione dell'ordinamento costituzionale, incidendosi 'soltanto' su alcune libertà fondamentali e non sull'assetto dei poteri statuali; l'A. riconosce, tra l'altro, che sia «funzionale all'emergenza una previsione tendenzialmente indeterminata» (189) delle situazioni in cui può dichiararsi lo stato d'emergenza e che lo spazio di un controllo della Corte costituzionale al riguardo, così come quello sull'adeguatezza delle ipotetiche misure emergenziali, sia limitato, trattandosi di valutazioni politiche. Ciò pare sufficiente a porre in evidenza gli enormi ed inaccettabili rischi per le libertà fondamentali che una siffatta 'clausola d'emergenza costituzionalizzata' comporterebbe, sia pure da introdursi con una maggioranza qualificata e per periodi di tempo limitati, come si propone (*ivi*, 191). Per una critica di proposte analoghe avanzate in dottrina – cfr. in part. M. DONINI, *Il diritto penale di fronte al "nemico"*, cit., 774 – sia consentito rinviare ancora al nostro *Diritto penale "del nemico" e "di lotta"*, cit., 288.

li[13], di cui non vi è traccia nella nostra Legge fondamentale, che – sia detto anche in riferimento al primo percorso sottoposto a critica – a differenza di altri ordinamenti e della stessa Convenzione europea dei diritti dell'uomo non prevede alcuna clausola che autorizzi la sospensione eccezionale della validità di alcuni principi. E va sottolineato che, laddove, come in questa ipotesi, la Costituzione preveda garanzie più elevate, esse devono prevalere sulla CEDU, dato che, secondo l'art. 53 della stessa, dalla CEDU non possono derivare limitazioni di diritti fondamentali maggiori di quelle previste negli ordinamenti dei singoli Stati parte.

Il terzo percorso è quello più insidioso, perché più difficile da contrastare. È quello ormai ricorrente, non solo in materia di terrorismo: l'affievolimento 'realistico', pragmatico, postmoderno dei principi, che ne dissimula il sostanziale svuotamento sotto le spoglie di una concreta

[13] R. BARTOLI, *Lotta al terrorismo internazionale*, cit., 183 ss., secondo cui nel nostro ordinamento sarebbe inammissibile uno stato d'emergenza "assoluto", che coinvolgesse, cioè, anche l'organizzazione dei poteri costituzionali, ma sarebbe, invece, implicitamente consentito uno stato d'emergenza "relativo", che implicherebbe 'solo' la sospensione di diritti e libertà della persona. «Quando la clausola di emergenza non è destinata a incidere sull'organizzazione costituzionale del potere limitandosi a sospendere alcune libertà, … non sembra vi sia la necessità di una espressa previsione di tale clausola» (183). Si tratterebbe, infatti, 'solo' di incidere, ad esempio, sul diritto all'integrità fisica, sull'inviolabilità del domicilio, sulla libertà di manifestazione del pensiero, sul principio di responsabilità penale personale, di offensività, sul diritto a trattamenti contrari al senso di umanità, e così via! Peraltro, l'Autore fa salvi i diritti umani "assoluti", citando «il divieto di arbitraria limitazione della libertà personale come anche il principio del giusto processo» (185). La stessa distinzione tra i diritti umani 'derogabili' ed inderogabili' è effettuata in modo arbitrario e, dunque, eversivo dei principi costituzionali, in un contesto normativo in cui l'art. 2 Cost. "riconosce e garantisce i diritti inviolabili dell'uomo". L'unica conferma, asseritamente "inequivocabile", dell'ammissibilità di uno stato d'eccezione implicito, l'Autore la rinviene nel dato per cui la Corte costituzionale, negli anni Ottanta del secolo scorso, avrebbe, in particolare in un'unica, nota sentenza (Corte cost., sent. 1 febbraio 1982, n. 15), ammesso la necessità di un giudizio di ragionevolezza adeguato alla situazione emergenziale. Si tratta di una base alquanto esile per asserzioni così gravi in rapporto alla vigenza dei principi costituzionali, che non possono fondarsi su controvertibili congetture dottrinali, elaborate a partire da una singola pronuncia della Corte costituzionale; oltretutto, in tal modo si finisce per ridurre la portata dei principi costituzionali a ciò che in proposito è stato riconosciuto dalla Corte, il cui atteggiamento, talora, di *self-restraint* conservatore è ben noto.

attuazione parziale, bilanciata con vaghe esigenze di 'sicurezza' e di 'tutela delle vittime'. Anche in questo caso, il preteso realismo si converte in un'affermazione prescrittiva, legittimante, con cui parte della dottrina, anziché porsi quale istanza di controllo critico dell'esercizio del potere punitivo, torna ad assumere l'antico ruolo di consigliere del principe o si rassegna alla politica criminale dominante; e, quindi, rinuncia a difendere le conquiste di civiltà sancite nella nostra Costituzione, le categorie della dommatica e la loro funzione di garanzia, e si converte in mera esegesi dell'esistente, lasciando residuare un angusto spazio critico solo nel rapporto con la giurisprudenza. È principalmente con tale orientamento che bisogna confrontarsi.

### *4. Un terreno nevralgico: la punibilità di accordi ed atti preparatori*

Un fondamentale terreno di confronto è quello della criminalizzazione del mero accordo e di remoti atti preparatori, caratteristica della normativa antiterrorismo[14].

Sul piano politico-criminale, sono diffuse due argomentazioni volte a legittimare tale anticipazione di tutela. La prima fa leva sulla funzione (special)preventiva del diritto penale: il commiato dalla teoria retributiva comporterebbe un orientamento del diritto penale alla prevenzione di condotte di reato, quindi ad intervenire appena possibile, ben prima che esse si realizzino[15]. Ma il dato per cui la pena deve tendere alla prevenzione generale e speciale – in senso positivo, cioè volto all'integrazione sociale[16] – non implica affatto che essa debba intervenire prima che sia stata posta in essere almeno una messa in pericolo reale, concreta, imminente di beni giuridici, come, d'altro canto, impongono i principi

[14] Sull'evoluzione della normativa interna in materia e sul rapporto con gli atti normativi europei ed internazionali, cfr. per tutti V. MASARONE, *Politica criminale e diritto penale nel contrasto al terrorismo internazionale. Tra normativa interna, europea ed internazionale*, Napoli, 2013, 117 ss., 209 ss.

[15] Descrive, in chiave critica, un tale diffuso orientamento W. HASSEMER, *Sicurezza mediante il diritto penale*, cit., 15 ss.

[16] Sulla pena come integrazione sociale, cfr. per tutti S. MOCCIA, *Il diritto penale tra essere e valore. Funzione della pena e sistematica teleologica*, Napoli, 1992, 83 ss.

costituzionali di offensività e di *extrema ratio*: principi legati ad una visione dei rapporti tra individuo e diritto penale volta all'integrazione sociale, anziché ad un soverchiante intervento statuale di stampo neutralizzante, fino all'estremo dello "psicoreato" di orwelliana memoria.

In particolare, il primato della persona, secondo la nostra Costituzione, comporta che il diritto penale debba intervenire soltanto quando ciò risulta strettamente necessario: cioè almeno in presenza di un pericolo concreto ed attuale per beni giuridici altrui. Fino ad allora, vi è un ampio spazio per una prevenzione extrapenale, che comprenda controlli e sanzioni meno invasivi. Invece, la criminalizzazione di remoti atti preparatori e del mero accordo trasforma il diritto – e il procedimento – penale in *prima ratio* del controllo di polizia o dei servizi di sicurezza: l'elemento investigativo (captazione di discorsi estremisti, intercettazione telematica della frequentazione di siti internet fondamentalisti, informativa circa la frequenza di un corso di arti marziali o l'acquisto di perossido di idrogeno concentrato, *id est* acqua ossigenata) viene elevato a fatto punibile e legittima, magari, la custodia cautelare in carcere. Ecco il panpenalismo: sembra che persino davanti ai primi, lontanissimi segnali di una futura, possibile preparazione di atti terroristici non vi sia altra risposta che il carcere.

Una seconda argomentazione politico-criminale diffusa in dottrina ed impiegata dalla stessa Corte costituzionale[17], è quella secondo cui il principio di proporzione consentirebbe, in relazione alla tutela di beni fondamentali, l'anticipazione della tutela penale ad atti remoti rispetto all'offesa[18]. Certamente, risulta conforme a proporzione anticipare la

[17] Corte cost., sent. 10-11 luglio 1991, n. 333, in *Riv. it. dir. proc. pen.*, 1992, 295-296.

[18] Cfr., ad es., in rapporto ai reati di pericolo astratto, D. PULITANÒ, *La formulazione delle fattispecie di reato: oggetti e tecniche*, in AA.VV., *Beni e tecniche della tutela penale. Materiali per la riforma del codice*, a cura del C.R.S., Milano, 1987, 35; in rapporto alla prospettata legittimità di fattispecie di attentato, al di sotto della soglia del tentativo, per la tutela della "personalità dello Stato", G. MARINUCCI, E. DOLCINI, *Corso di diritto penale*, *1. Nozione, struttura e sistematica del reato*, Milano, 1995, p. 149 ss., 244, e 231; v. anche G. FIANDACA, *Il "bene giuridico" come problema teorico e come criterio di politica criminale*, in AA.VV., *Bene giuridico e riforma della parte speciale*, a cura di A. M. STILE, Napoli, 1985, 50 ss.; per una puntuale critica del percorso argomentativo descritto nel testo, N. MAZZACUVA, *Il disvalore di evento nell'illecito penale*,

tutela penale di beni fondamentali alla messa in pericolo attuale e concreta; ma non si può ammettere che tali beni possano essere, in quanto primari, tutelati anche a fronte di condotte inoffensive o di meri propositi criminosi! Il principio di offensività dovrebbe fungere, anche qui, da argine ad una prevenzione illimitata, ed invece viene surrettiziamente svuotato, come si è accennato. Del resto, appare evidente il paralogismo insito nell'affermazione per cui, per la tutela di beni fondamentali, la proporzione consente di derogare alla necessaria offensività; allora, per la tutela di quegli stessi beni fondamentali, si potrebbe, in virtù della proporzione, derogare pure alla personalità della responsabilità penale o alla stretta legalità! Ciò equivarrebbe a riabilitare incredibilmente *crimina* e *poenae extraordinariae*, secondo il premoderno brocardo «in delictis atrocissimis propter criminis enormitatem jura transgredi licet»[19].

Nel dibattito intorno alla punibilità di atti preparatori, assume un ruolo rilevante la dommatica. Infatti, non diversamente da altri principi, quello di necessaria offensività, fondamentale riferimento teleologico di una politica criminale conforme a Costituzione, richiede un'opera di formalizzazione e concretizzazione, che è compito della dommatica, *sub specie* teoria generale del reato, realizzare[20]. Un tale faticoso lavoro di elaborazione teorica può contribuire a fornire strumenti concettuali atti ad orientare la giurisprudenza, rendendo così 'giustiziabile' il principio di offensività, non diversamente da quanto avviene in relazione agli altri principi[21].

---

Milano, 1983, 191, che propone, invece, di partire dalla ricognizione delle tecniche di tutela compatibili con il principio di offensività, dando spazio al criterio del rango del bene solo nell'ambito così previamente delineato.

[19] Su questa dottrina carpzoviana, cfr. S. MOCCIA, *Carpzov e Grozio. Dalla concezione teocratica alla concezione laica del diritto penale*, 2ª ed., Napoli, 1988, 18 ss., spec. 36.

[20] Cfr. S. MOCCIA, *L'odierna funzione di 'controllo' e 'orientamento' della dottrina*, in *Criminalia*, 2013, 409 ss.

[21] Si pensi, ad esempio, in rapporto al principio di personalità della responsabilità penale, ai concetti dommatici di colpa 'presunta', responsabilità 'di posizione', responsabilità oggettiva espressa o 'occulta', che servono a definire e, quindi, a denunciare tecniche legislative o orientamenti giurisprudenziali in contrasto con quel principio. Allo stesso scopo mirano, da sempre, in rapporto al principio di offensività, i concetti di

Sul piano della teoria generale del reato, si distingue, dunque, corrispondentemente alla distinzione tra materialità ed offensività, tra i requisiti che un fatto tipico deve presentare perché possa dirsi conforme a ciascuno di essi. La teoria del reato non ha, infatti, soltanto una funzione descrittiva degli elementi del reato previsti dal legislatore, ma ha pure una funzione prescrittiva, costituzionalmente orientata, nei confronti di quest'ultimo, prima che del giudice[22].

Ebbene, sul piano della tipicità, la sussistenza di una condotta umana percepibile dall'esterno e non riducibile alla mera *cogitatio* soddisfa soltanto il principio di materialità. Ma quando si parla di un diritto penale del fatto conforme a Costituzione non ci si accontenta di questo, bensì si richiede anche che la condotta esteriormente percepibile leda o ponga in pericolo un bene giuridico. Ad esempio, la mera dichiarazione della propria volontà criminosa è qualcosa di non meramente interiore, non è più nuda *cogitatio*; ma certamente è sideralmente lontana dal mettere in pericolo un bene giuridico. Anche l'accordo criminoso è, se si vuole, una manifestazione esteriore collettiva di previe *cogitationes*; esso soddisfa – solo – le esigenze poste dal principio di materialità, ma è ancora troppo distante dall'offesa e precede gli stessi atti preparatori.

Esistono, inoltre, infinite condotte neutre – come noleggiare un'auto, comprare acqua ossigenata o fertilizzanti, allenarsi nelle arti marziali, frequentare scuole di volo, visitare siti internet di mera propaganda estremista o fondamentalista, procurarsi mappe di determinati luoghi, informarsi su armi ed esplosivi e sul loro uso senza possederli – che possono costituire atti preparatori… di atti preparatori di reati (!) e che, in quanto tali, soddisfano solo l'esigenza di materialità, ma sono lontanissimi dal porre veramente, concretamente, attualmente in pericolo beni giuridici.

---

pericolo astratto o presunto, delitti di attentato, reati di opinione, e così via; peraltro, una preoccupante differenza dall'esempio precedente risiede nel riflusso dottrinale che, dopo la stagione del primato del teleologismo costituzionalmente orientato, ha ripreso, già sul finire degli anni Settanta del secolo scorso, a legittimare quelle tecniche di tutela.

[22] Cfr. per tutti F. BRICOLA, *Teoria generale del reato*, in *Nss. D. I.*, XIX, Torino, 1974, 12, 20.

Basterebbe far riferimento ad una chiara distinzione dommatica – riconducibile a quella politico-criminale tra i principi costituzionali di materialità ed offensività – tra condotta esteriormente percepibile e fatto offensivo, per sgomberare il campo da orientamenti legislativi, dottrinali e giurisprudenziali che legittimano la punizione del mero accordo[23], di condotte neutre o di remoti atti preparatori.

Della dommatica dell'offensività – certamente 'scomoda', perché, attraverso categorie generali, fissa garanzie e indica limiti al legislatore ed all'interprete – fa parte anche, da sempre, seppure in maniera non incontroversa, la distinzione tra atti preparatori ed esecutivi e quella, asimmetrica rispetto alla prima, tra reati di pericolo e reati di danno. Anche stavolta, trascurare l'asimmetria tra le due distinzioni conduce a legittimare la punibilità di condotte che non dovrebbero ritenersi punibili: non è sufficiente affermare che una certa fattispecie costituisce un reato di pericolo – senza talora neppure precisare se astratto o concreto – per stabilirne la conformità al principio di offensività. Ogni atto preparatorio, per quanto lontanissimo dall'esecuzione, crea o aumenta il lontano pericolo di un'offesa! Tuttavia, autorevole dottrina richiede condivisibilmente che il pericolo venga visto non in rapporto alla possibile continuazione della preparazione, bensì in rapporto alla realizzazione del fatto offensivo di beni giuridici, e che, dunque, debbano risultare punibili, se non le sole condotte esecutive, quantomeno solo quegli atti con cui ci si approssima all'esecuzione[24]. Punibili dovrebbero essere, dunque, soltanto quegli atti preparatori direttamente idonei all'offesa e prossimi all'esecuzione: non basta etichettare come 'pericoloso' un atto preparatorio per legittimarne la punibilità, o definire quale 'reato di pericolo' una fattispecie riferita ad atti lontanamente preparatori per salvarne la conformità al principio di offensività.

Tra gli effetti deleteri della criminalizzazione di meri atti preparatori vi può essere quello, ben noto, della soggettivizzazione della fattispe-

[23] Un esempio per tutti concerne la concezione della partecipazione quale mera "assunzione di un ruolo", su cui v. *infra*, par. 5.

[24] Cfr. C. FIORE, S. FIORE, *Diritto penale. Parte generale*, 4ª ed., Torino, 2013, 523 ss., 527-528, 530-531.

cie[25]: il disvalore del fatto rischia di imperniarsi sull'atteggiamento interiore, e ciò aumenta il potere discrezionale del giudice, che può orientarsi a precomprensioni fondate sul tipo d'autore. Per chi, ad esempio, frequenti abitualmente ambienti estremistici o, in particolare, fondamentalisti islamici, ma anche per quei soggetti che abbiano manifestato, magari solo in modo privato – ma comunque noto alle forze dell'ordine –, atteggiamenti ideologicamente estremistici o integralisti, il rischio di essere sottoposti a procedimenti penali e misure cautelari per condotte neutre, ma che possano essere interpretate come possibili atti preparatori, risulta certamente più elevato[26].

Un ulteriore inconveniente dell'anticipazione della tutela ad atti preparatori può consistere nell'indeterminatezza della fattispecie: quanto più ci si allontana dalla condotta attualmente e concretamente pericolosa, tanto più si amplia, tendenzialmente, il novero degli atti che potrebbero astrattamente condurre verso quella condotta. Quindi, un legislatore ossessionato dall'intento di intervenire penalmente per chiudere qualsiasi possibile spazio alla preparazione di fatti di terrorismo tenderà ad ampliare a dismisura la sfera del punibile. Anche sul punto, non devono esservi cedimenti dottrinali rispetto all'esigenza di una descrizione precisa della condotta tipica, né deleghe in bianco al 'diritto vivente' giurisprudenziale.

Peraltro, talora accade che il legislatore – influenzato da 'formanti' giurisprudenziali tipici della *common law* e recepiti nelle norme sovranazionali – proceda secondo moduli accentuatamente casistici, descrivendo magari accuratamente delle condotte preparatorie, ma senza alcun riguardo alla loro necessaria offensività: così, ad esempio, allorché assoggetta a pena la detenzione di precursori di esplosivi contenuti in un elenco, fra i quali sono compresi comuni fertilizzanti o persino l'ac-

[25] Sul tema, cfr. spec. N. MAZZACUVA, *Il disvalore di evento nell'illecito penale*, cit., *passim* e in particolare 24 ss. e 177 ss., sui rapporti tra soggettivismo e, rispettivamente, delitti di attentato e a consumazione anticipata.

[26] Così pure – in riferimento all'estensione della punibilità agli atti preparatori nella normativa antiterrorismo dei Paesi nordici – E.J. HUSABØ, *Die Kriminalisierung von terroristischen Straftaten und deren Vorbereitung in den nordischen Ländern – eine kritische Betrachtung*, in *ZStW*, 2012, 1167.

qua ossigenata in concentrazioni comunemente impiegate da dentisti e parrucchieri[27].

### *5. Associazione terroristica e finalità di terrorismo*

Poste tali premesse metodiche, politico-criminali e dommatiche, e passando ad una disamina delle figure di reato connesse al controllo del fenomeno terroristico, viene in rilievo in primo luogo la fattispecie associativa di cui all'art. 270 *bis* c.p.

Com'è ben noto, la dottrina penalistica è da sempre critica sulle fattispecie associative: anzitutto sul piano dell'offensività – perché attraverso esse si rende punibile il mero accordo, sia pur stabile ed organizzato –, ma anche in rapporto al principio di legalità, per l'indeterminatezza dei concetti di associazione e partecipazione, e sotto il profilo della personalità della responsabilità, per l'appiattimento delle responsabilità stesse, evidente specialmente nei c.d. maxiprocessi.

La fattispecie associativa funziona sempre (a) quale diffusore della responsabilità penale, in chiave di sospetto, nei confronti di chi non abbia partecipato alla commissione di alcun fatto di reato; (b) quale moltiplicatore artificiale della pena, fondato sulla pericolosità soggettiva, verso coloro che già devono rispondere di uno o più reati; (c) quale scorciatoia probatoria e, sempre sul piano processuale, (d) quale veicolo per l'applicazione di percorsi procedimentali speciali, con garanzie attenuate.

In materia di reati associativi politici, in particolare, si è posto da tempo in evidenza il rischio di punire la mera manifestazione associata di idee sovversive (art. 270 c.p.), eversive o terroristiche (art. 270 *bis* c.p.): in rapporto a queste ultime, si pensi alla controversia sul significato dell'espressione «si propongono il compimento di atti di violenza»[28].

In dottrina, la – fondatissima – critica verso i reati associativi si è andata negli ultimi tempi spegnendo; la rassegnata presa d'atto si tra-

[27] In proposito, v. *infra*, par. 6.

[28] Cfr. ad es. G. FIANDACA, E. MUSCO, *Diritto penale. Parte speciale*, I, 4ª ed., Bologna, 2007, 46-47.

sforma, così, in legittimazione dell'esistente. Ma vi è di più. L'idea – incompatibile con i principi di *extrema ratio*, determinatezza, frammentarietà, offensività – di fare 'terra bruciata' intorno alle associazioni criminali, punendo anche meri atteggiamenti interiori, appena dichiarati, di disponibilità e contiguità, si è tradotta – lasciando da parte il cosiddetto concorso 'esterno' – nell'impressionante espansione del concetto di partecipazione. Partecipe di associazione terroristica, come di qualsiasi altra associazione, è – secondo un'accezione cosiddetta 'organica', che fa leva sulla mera disponibilità[29] o sull'affiliazione[30] – già chi

[29] Cfr. G. TURONE, *Il delitto di associazione mafiosa*, Milano, 1995, 293 ss., 294, 301, secondo cui la «soglia minima di contributo partecipativo astrattamente ipotizzabile è, teoricamente, la mera manifestazione di *impegno* con cui il nuovo affiliato *mette a disposizione* del sodalizio le proprie energie»; «una siffatta disponibilità, infatti, costituisce essa stessa un contributo alla vita dell'ente». Quest'ultima asserzione contiene manifestamente un'inaccettabile presunzione di causalità del mero impegno o accordo, presente anche in Ass. Palermo, 16 dicembre 1988, Abbate e altri, in *Foro it.*, 1989, II, 82-83 (con nota di G. FIANDACA, F. ALBEGGIANI) – secondo cui non vi è dubbio che «la conclamata disponibilità costituisca essa stessa un contributo alla vita dell'ente, tale da ampliarne le potenzialità operative sul piano criminale» – e nella giurisprudenza conforme citata nella nota successiva.

[30] Cfr. Ass. Palermo, 16 dicembre 1988, Abbate e altri, cit. II, 82-83, secondo cui «la soglia minima di contributo ipotizzabile può anche consistere nel solenne giuramento col quale l'"uomo d'onore" aderisce consapevolmente al gruppo e al suo programma criminoso»; «diversamente opinando, nel caso di un imputato il quale confessi attendibilmente di essere membro del sodalizio criminoso, e di essersi messo, quindi, a disposizione del gruppo criminale, ma di non aver avuto ancora l'occasione di dare alcun contributo materiale alla vita dell'ente, si arriverebbe all'assurdo, malgrado il perfezionamento del vincolo associativo… di non poter ritenere sussistente il reato di cui all'art. 416 *bis* c.p.», *ivi*, 95. Fiandaca ed Albeggiani, nella nota poc'anzi citata, rilevano che sul concetto di partecipazione impiegato dalla Corte d'Assise grava il duplice rischio di aprire ad un diritto penale del tipo d'autore – vista la possibilità che al giuramento non segua alcuna condotta associativa – e di escludere la punibilità di contributi di soggetti che non abbiano prestato giuramento, ma altrettanto meritevoli di pena quali partecipi; cfr. *ivi*, 83-84. L'impostazione della Corte d'Assise di Palermo ha trovato conferma in Cass. pen., sez. I, 30 gennaio 1992, Abbate e altri, in *Foro it.*, 1993, II, 15 ed in tante altre decisioni della Corte di Cassazione, tra cui Cass. pen., sez. I, 11 dicembre 1992, Oro, in *Cass. pen.*, 1995, 45; Cass. pen., sez. I, 28 settembre 1998, Bruno, in *Cass. pen.*, 1999, 2510; Cass. pen., sez. II, 28 gennaio 2000, Oliveri, in *Cass. pen.*, 2001, 844; Cass. pen., sez. I, 1 marzo 2002, Vento, in *Giur. it.*, 2004, 1481-1482.

s'impegna ad assumervi un ruolo[31]. Si può aggiungere il termine "seriamente", si può addurre la pretesa forza psicologica di vincoli interiori derivanti dall'accordo e dall'impegnarsi verso una struttura gerarchica, ma la sostanza non cambia: si finisce per rendere punibile il mero accordo criminoso[32].

Infatti, applicando il concetto 'organico' di partecipazione, è stato possibile infliggere la pena della reclusione, in qualche recente sentenza, a chi si era soltanto detto pronto ad unirsi ai fratelli islamici nella *jihad*[33]. Ebbene, a me pare che nessun obiettivo di 'lotta' al terrorismo possa giustificare la reclusione di un giovane immigrato tra i cinque e i dieci anni, *ex* art. 270 *bis* co. 2 c.p. – e, quindi, il rischio di rovinargli la vita per sempre – sulla base di una mera affermazione di 'disponibilità', senza che vengano violati elementari principi di civiltà giuridica; e credo che una dottrina che non si ponga questo problema mostri, sotto tale profilo, scarso senso di umanità.

---

[31] Cfr. spec. G. DE FRANCESCO, *Associazione per delinquere e associazione di tipo mafioso*, in *Dig. disc. pen.*, I, Torino, 1987, 291, 293 ss.; ID., Societas sceleris. *Tecniche repressive delle associazioni criminali*, in *Riv. it. dir. proc. pen.*, 1992, 107 ss.; A. INGROIA, *L'associazione di tipo mafioso*, Milano, 1993, 39 ss.; L. DE LIGUORI, *Concorso e contiguità nell'associazione mafiosa*, Milano, 1996, 60 ss., 65, 69 nota 14; V.B. MUSCATIELLO, *Il concorso esterno nelle fattispecie associative*, Padova, 1995, 140 ss.

[32] Per più ampie considerazioni critiche in argomento sia consentito rinviare al nostro *Associazione per delinquere, Associazione di tipo mafioso, Scambio elettorale politico-mafioso*, in S. MOCCIA (a cura di), *Delitti contro l'ordine pubblico*, Napoli, 2007, 273 ss., 298 ss., 424 ss.

[33] Cfr. Cass. pen., sez. V, sent. 02.10.2008, n. 39430, Rabei e altro, in *www.iusexplorer.it*. La Cass., in relazione al ricorrente Yahia, cita, nel "rilevato in fatto", quale elemento probatorio cui fa "essenzialmente riferimento" la sentenza di appello, i «colloqui, captati mediante intercettazioni ambientali, tra il Rabei ed il più giovane Yahia, ritenuti dimostrativi… della ottenuta adesione del secondo» ad un'associazione terroristica. Nel "considerato in diritto" la Cass. motiva il rigetto del ricorso rilevando come sia *jus receptum*, in materia di reati associativi, che ai fini della punibilità a titolo di partecipazione sia «soltanto necessaria e sufficiente la dimostrazione che il soggetto abbia dato la propria seria e consapevole disponibilità a contribuire […] indipendentemente dalla circostanza che il contributo venga poi effettivamente richiesto e fornito». Su ulteriori pronunce in cui l'associazione terroristica viene ridotta a mero accordo, ossia a reciproca "disponibilità", cfr. criticamente F. FASANI, *Terrorismo islamico e diritto penale*, Milano, 2016, 249 ss.

Un'altra disposizione centrale nella normativa antiterrorismo che si pone in tensione con i principi costituzionali di offensività e legalità è l'art. 270 *sexies* c.p., in tema di condotte con finalità di terrorismo[34]. Esso incide sull'applicabilità di fattispecie associative qualificate (come l'art. 270 *bis* c.p.) o di eccezionali anticipazioni della tutela (ad es., artt. 270 *quater* e *quinquies* c.p.) o della circostanza aggravante ad effetto speciale di cui all'art. 1 d.l. n. 625/1979, conv. in l. n. 15/1980. Tale applicabilità dipende da una definizione che fa riferimento a condotte che «possono» arrecare «grave danno» ad un Paese o ad un'organizzazione internazionale e sulla finalità alternativa di

> intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale.

Ebbene, il primo problema posto da tale disposizione consiste nel fatto che, diversamente dalla definizione contenuta nella decisione-quadro in tema di terrorismo del 2002, modificata nel 2008, l'art. 270 *sexies* c.p. si applica a qualsiasi condotta punibile; basta un mero danneggiamento, una violenza privata, una resistenza a pubblico ufficiale, etc.

Certo, occorre che si tratti di condotta che possa arrecare un grave danno ad un Paese, etc. Ma il concetto di "possibilità" è notoriamente molto più ampio e generico di quello di probabilità o di idoneità. E il grave danno potrebbe abbracciare certamente il danno economico e quello di immagine, che pure può avere riflessi 'sui mercati', come si suol dire[35].

---

[34] Sul punto, cfr. i puntuali rilievi di V. MASARONE, *Politica criminale e diritto penale nel contrasto al terrorismo internazionale*, cit., 209 ss., con ulteriori riferimenti bibliografici.

[35] Sulle incertezze giurisprudenziali, oltre che dottrinali, cui ha dato luogo la formula legislativa del «grave danno», fino a comprendere il danno patrimoniale e quello di immagine, cfr. Cass. pen., sez. VI, sent. 15.05.2014, n. 28009, Alberto ed altri, in *www.iusexplorer.it*, considerato in diritto, punto 4.3: «Per l'identificazione del danno si è spaziato tra la dimensione patrimoniale (come si è fatto, nel caso di specie, anche dai

Inoltre, basta la finalità di «costringere pubblici poteri» a fare od omettere qualunque cosa o, ad esempio, di «destabilizzare» strutture economiche o sociali. Una tale definizione comprende, quindi, qualsiasi protesta sociale violenta o turbolenta nei confronti di istituzioni pubbliche o organizzazioni internazionali, ad esempio in relazione alla costruzione di infrastrutture quali una linea ferroviaria ad alta velocità (TAV) o all'insediamento di basi NATO; è sempre "possibile" che ne derivi un "grave danno" per lo Stato o un'istituzione internazionale.

Effettivamente si è tentato di applicare l'art. 270 *sexies* c.p. a movimenti sociali di opposizione e protesta violenta come quello 'no-TAV'; e la prevedibile obiezione ai rilievi critici appena mossi è che la giurisprudenza di Cassazione ha negato la configurabilità della finalità di terrorismo, interpretando in senso conforme al principio di offensività l'art. 270 *sexies* c.p.[36]. Agli entusiasti del 'diritto vivente' di matrice giurisprudenziale occorre far notare, tuttavia, che i consociati hanno diritto di vivere in un Paese nel quale le sfere di libertà siano stabilite, con precisione e conformemente al principio di offensività, dalla legge, e non rimesse agli umori della giurisprudenza; un Paese nel quale non si debba attendere in carcere – in custodia cautelare – e, comunque, dopo anni di estenuante sottoposizione a processo, di sapere dalla Cassazione se la propria condotta era lecita. Cassazione la cui pronuncia, come tutti sanno, non costituisce un precedente vincolante, che metta al riparo i consociati da future pene detentive o custodie cautelari in carcere; e, comunque, il compito di fissare conformemente al principio di offensività l'ambito del punibile non dovrebbe spettare – in un sistema

Giudici della cautela) ed altro genere di prospettazioni (ad esempio, sempre ad opera dei Giudici *a quibus*, relativamente al danno da immagine)». Tali incertezze non sono, dunque, paventate artificiosamente in astratte elaborazioni dottrinali, ma incidono concretamente sulla libertà personale di persone in carne ed ossa, che a seconda delle diverse interpretazioni giudiziali finiscono in (custodia cautelare in) carcere o vengono liberate. Peraltro, nella stessa sentenza, al punto 4.4 del considerato in diritto, la Corte di Cassazione propone il riferimento, tutt'altro che preciso e pregnante, del "grave danno" a beni giuridici vaghi quali «il sereno svolgimento della vita pubblica, il fisiologico esercizio del potere pubblico, la stabilità […] delle istituzioni».

[36] Cass. pen., sez. I, sent. 16.07.2015, n. 47479, Alberti ed altri, in *www.iusexplorer.it*, considerato in diritto, punti 3.2 ss.

fondato sul principio di legalità – alla Cassazione, ma incombere sul legislatore[37].

### *6. Singole ipotesi di punibilità di atti preparatori non 'associati'*

Com'è noto, con il d.l. 27 luglio 2005, n. 144, conv. con modif. con l. 31 luglio 2005, n. 155[38], sono stati introdotti gli artt. 270 *quater* c.p., in tema di arruolamento con finalità di terrorismo, e 270 *quinquies* c.p., in tema di addestramento ad attività con finalità di terrorismo; entrambe le norme sono state ampliate dal recente d.l. 18 febbraio 2015, n. 7, conv. con modif. con l. 17 aprile 2015, n. 43. Inoltre, quest'ultimo decreto legge convertito ha introdotto l'art. 270 *quater*.1 c.p., organizzazione di trasferimenti per finalità di terrorismo.

All'elenco delle ipotesi di punibilità di atti preparatori vanno aggiunti l'art. 280 c.p., «attentato per finalità terroristiche o di eversione», e l'art. 280 *bis* c.p., «atto di terrorismo con ordigni micidiali o esplosivi», introdotto dall'art. 3 l. 14 febbraio 2003, n. 34. Anche la punibilità del finanziamento del terrorismo, «indipendentemente dall'effettivo uti-

[37] Non è possibile affrontare in questa sede l'ampio e complesso tema dei rapporti tra la necessaria determinatezza della legge penale e il ruolo del 'diritto vivente' giurisprudenziale. Mi limito a riportare due autorevoli e condivisibili giudizi sul punto: «La precisione conferita alla norma dall'opera della giurisprudenza non può ovviare in alcun modo alla congenita imprecisione del testo legislativo», G. MARINUCCI, E. DOLCINI, *Corso di diritto penale. 1. Le fonti. Il reato: nozione struttura e sistematica*, 3ª ed., Milano, 2001, 83; il riferimento al diritto vivente, «oltre ad essere suscettivo di applicazioni troppo duttili e perciò facilmente manipolabili, attribuisce un ruolo eccessivo alla giurisprudenza ordinaria, che viene così caricata del ruolo di supplire alle deficienze del legislatore; e, cosa ancora più grave, esso consente alla Corte [costituzionale] di pretermettere l'esame diretto del grado di tassatività delle norme considerate nella loro formulazione testuale», G. FIANDACA, E. MUSCO, *Diritto penale. Parte generale*, 6ª ed., Bologna, 2010, 79.

[38] Per un commento alle innovazioni di diritto penale sostanziale ivi contenute, v. fra gli altri A. VALSECCHI, *Le modifiche alle norme incriminatrici in materia di terrorismo*, in R.E. KOSTORIS, F. VIGANÒ (a cura di), *Il nuovo 'pacchetto' antiterrorismo*, Torino, 2015, 3 ss., con ult. rif. bibl.; sia consentito rinviare pure al mio *Considerazioni critiche intorno al d.l. antiterrorismo, n. 7 del 18 febbraio 2015*, in *Dir. pen. cont.*, 31 marzo 2015.

lizzo dei fondi», introdotta, nel nuovo art. 270-*quinquies*.1 c.p., dall'art. 4 co. 1 lett. a l. 28 luglio 2016, n. 153, abbraccia atti meramente preparatori. Ma va pure tenuta presente la previsione, con il citato d.l. n. 7/2015, conv. con modif. con l. n. 43/2015, delle contravvenzioni di detenzione abusiva di precursori di esplosivi, art. 678 *bis* c.p. e di omessa denuncia di furto o sparizione di precursori di esplosivi, art. 679 *bis* c.p.

Si tratta chiaramente di una criminalizzazione a tappeto di atti preparatori e di condotte enormemente lontane dalla concreta offesa di beni giuridici. Non vi è paralogismo relativo alla proporzione che tenga: la violazione dei principi di *extrema ratio* ed offensività ed il rischio di punire condotte neutre, andando a caccia di atteggiamenti interiori, ossia di tipi d'autore estremisti o integralisti, sono fin troppo manifesti[39].

Ad esempio, l'arruolamento di cui all'art. 270 *quater* c.p., punibile con la reclusione da sette a quindici anni (!), è descritto dal legislatore con una tautologia: «Chiunque arruola una o più persone». Ma che cosa significa arruolare: basta l'istigazione o l'accordo criminoso? La definizione della condotta punibile è rimessa al diritto giurisprudenziale[40].

La «finalità di terrorismo», in questa come in altre fattispecie – ad esempio, quella di addestramento – rischia, in ragione della struttura del precetto, di perdere nell'applicazione giudiziale pure quel connotato

[39] In senso nettamente critico verso l'esasperata anticipazione di tutela ad atti preparatori cui si assiste nei sistemi penali europei, per tutti, C. ROXIN, *Dalla dittatura alla democrazia. Tendenze evolutive nel diritto penale e processuale penale tedesco*, in A.M. STILE (a cura di), *Democrazia e autoritarismo nel diritto penale*, Napoli, 2011, 74 ss.; P. ASP, N. BITZILEKIS, S. BOGDAN, T. ELHOLM, L. FOFFANI, D. FRÄNDE, H. FUCHS, M. KAIAFA-GBANDI, J. LEBLOIS-HAPPE, A. NIETO MARTÍN, C. PRITTWITZ, H. SATZGER, E. SYMEONIDOU-KASTANIDOU, I. ZERBES, *European criminal policy initiative. Manifesto sulla politica criminale europea*, in *Riv. it. dir. proc. pen.*, 2010, 1268-1269. Per un diverso ordine di idee, v. nella dottrina italiana spec. F. MANTOVANI, *Il diritto penale del nemico, il diritto penale dell'amico, il nemico del diritto penale e l'amico del diritto penale*, cit., 484; F. VIGANÒ, *Terrorismo, guerra e sistema penale*, cit., 691-692.

[40] Significativa, in proposito, Cass. pen., sez. I, sent. 09.09.2015, n. 40699, Elezi ed altro, in *www.iusexplorer.it*, punto 3 del "considerato in diritto", in cui, respingendo un precedente contrario orientamento della Cassazione, si afferma che "arruolamento" significhi semplicemente raggiungimento di un "serio accordo"; con tale accordo si raggiungerebbe infatti la soglia del pericolo "in tesi presunto", punto 3.1. Sul punto cfr. pure F. FASANI, *Terrorismo islamico e diritto penale*, cit., 346 ss.

oggettivo, sia pur insufficiente, che è presente nell'art. 270 *sexies* c.p., in tema di «condotte con finalità di terrorismo»: infatti, nulla garantisce che il concetto di arruolamento punibile venga interpretato restrittivamente, nel senso che tale sia soltanto quello che «può cagionare grave danno» allo Stato, etc.

Nell'art. 270 *quater.*1 c.p., la condotta di «organizzare, finanziare e propagandare viaggi in territorio estero finalizzati al compimento delle condotte» con finalità di terrorismo – punibile con la reclusione da cinque ad otto anni – abbraccia pure la mera propaganda volta ad intraprendere atti preparatori, punibile anche se nessuno risponde positivamente, foss'anche solo chiedendo il prezzo del biglietto!

L'art. 270 *quinquies* c.p., in tema di addestramento, rende punibili con la reclusione da cinque a dieci anni, tra le altre condotte, anche quella di chi non "addestra", ma si limita a fornire istruzioni – magari pubblicandole su un sito internet – su armi o esplosivi, ma anche su «ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali». In una locuzione così ampia sono comprese istruzioni sull'uso di cesoie per tagliare reti o fili elettrici, su mosse di arti marziali, su come affilare coltelli, e così via. Non è richiesta un'effettiva idoneità delle istruzioni fornite[41]; ma, pur interpretando la disposizione in tal senso, rimane l'anticipazione della tutela ad atti lontanamente preparatori.

Per quanto riguarda la persona addestrata, è punibile anche quella… non addestrata, qualora, «avendo acquisito, anche autonomamente, le istruzioni per il compimento» dei predetti atti, ponga «in essere comportamenti univocamente finalizzati alla commissione delle condotte» con finalità di terrorismo[42]: chiunque visiti un sito internet, vi legga

[41] Correttamente Cass. pen., sez. VI, sent. 20.07.2011, n. 29670, Garouan, punto 5.3 ss., 7, in *www.iusexplorer.it*, affermava, in rapporto alla formulazione allora vigente dell'art. 270 *quinquies* c.p., che l'addestramento dovrebbe richiedere un processo interattivo di apprendimento, idoneo a trasmettere conoscenze ed abilità, ben al di là del mero fornire istruzioni. Su tale pronuncia, v. in part. E. FRONZA, *Tutela penal anticipada y normativa antiterrorismo en el ordenamiento italiano*, in K. AMBOS, E. MALARINO, C. STEINER (a cura di), *Terrorismo y derecho penal*, Berlin, 2015, 261 ss.

[42] R. WENIN, *L'addestramento per finalità di terrorismo alla luce delle novità introdotte dal d.l. 7/2015*, in *Dir. pen. cont.*, 3 aprile 2015, 13 ss., pone bene in evidenza come il soggetto meramente "istruito" non sia necessariamente "addestrato" e come,

delle istruzioni ed esca di casa per acquistare il coltello da affilare o le cesoie rischia di rendersi punibile. In assenza di qualsiasi riferimento legislativo all'idoneità degli atti ed alla loro prossimità all'esecuzione, la libertà dell'individuo è appesa al termine «univocamente» che, se da un lato è suscettibile di un'interpretazione teleologicamente orientata al principio di offensività, che richieda atti idonei e prossimi all'esecuzione, dall'altro, conformemente all'evidente *ratio legis* dell'anticipazione della tutela, può essere interpretato anche in chiave soggettiva, ossia come mera direzione inequivoca della volontà; e l'interpretazione rischia di dipendere, ancora una volta, dal tipo d'autore, 'no global', 'disobbediente' o 'integralista'.

La stessa esasperata anticipazione della tutela si ritrova nel reato di detenzione dei precursori di esplosivi elencati nell'allegato I del regolamento (CE) n. 98/2013: fra le sostanze ivi menzionate si trovano l'acqua ossigenata – in concentrazioni finora comunemente usate da dentisti e parrucchieri – ed alcuni fertilizzanti, ma anche il liquido contenuto nelle batterie di ogni autoveicolo. Anche stavolta, il rischio di punire tipi d'autore sulla base di condotte neutre, sospettando finalità di terrorismo, non può essere escluso. La punibilità pure dell'omessa denuncia di furto o sparizione di possibili precursori di esplosivi risulta francamente sconcertante, per la probabile assoluta ineffettività della norma o, laddove venga applicata, per l'esasperato rigore repressivo insito nella punizione di colui che non denunci di aver smarrito la bottiglia di acqua ossigenata o di concime.

A completamento del quadro relativo all'anticipazione di tutela vanno citate le norme sul tentativo. Certo, esse non sono applicabili a chi tenta di procurarsi precursori realizzando la relativa contravvenzione; in ciò gli ansiosi sostenitori di una criminalizzazione di atti preparatori di ulteriori atti preparatori dovrebbero vedere una grave lacuna, perché chi si procura precursori di precursori allo scopo di produrre precursori nel proprio laboratorio domestico non è punibile… Ma, invece, in astratto è configurabile il tentativo di arruolamento, di addestramento o mera 'istruzione', di propaganda di viaggi in Siria o magari nella Turchia

d'altro canto, l'ulteriore requisito normativo costituito da un qualsiasi comportamento successivo, soggettivamente diretto ad atti terroristici, non basti ad assicurare la conformità al principio di offensività.

orientale. Si obietterà – giustamente! – che giungere a punire il tentativo del mero accordo o di meri atti preparatori sarebbe un'esasperazione dell'anticipazione della tutela penale ancor più incompatibile con il principio di offensività di quanto non lo sia già la punizione di accordi o atti preparatori 'consumati'. Ma quando si accetta una legislazione confliggente con i principi costituzionali, affidando la difesa di tali principi all'interpretazione, ci si consegna alla discrezionalità giudiziale, che talvolta si orienta nel senso di assecondare tendenze repressive di stampo emergenziale: è il caso proprio del tentativo di arruolamento[43].

Bisogna tener presenti pure la punibilità dell'istigazione privata, art. 302 c.p., del mero accordo, art. 304 c.p., nonché dell'istigazione pubblica e dell'apologia di «delitti di terrorismo», art. 414 co. 4 c.p., riferibili non solo a fatti offensivi di beni giuridici, ma anche a remoti atti preparatori: si pensi al mero accordo, all'istigazione – privata o pubblica – ed all'apologia riferiti al reclutamento, all'addestramento e all'istruzione. La punibilità rischia di estendersi qui alla mera manifestazione di pensiero inquadrabile anche vagamente in un contesto ideologico fondamentalistico, 'radicale' o 'eversivo'. A tale proposito, mi domando se dire "le cesoie servono a tagliare le reti" configuri un'istigazione a delinquere tagliando le reti o un'istruzione punibile *ex* art. 270 *quinquies* c.p. o un'istigazione all'istruzione, pure punibile secondo il combinato disposto degli artt. 302 o 414 c.p. e 270 *quinquies* c.p.; ma sicuramente problemi simili susciteranno l'interesse e le risposte – naturalmente differenziate e foriere di ulteriore incertezza giuridica – di qualcuno dei solerti e compiaciuti esegeti che alimentano l'attuale, ipertrofica produzione di cattivo giornalismo penalistico 'usa e getta', pronti a scrivere al riguardo un contributo pieno di acribiche distinzioni, probabilmente di taglio casistico, magari a commento dell'ennesima, salvifica pronuncia della giurisprudenza, specie di Cassazione;

[43] Cass. pen., sez. I, sent. 09.09.2015, n. 40699, cit., punto 3.1 del "considerato in diritto", ritiene infatti punibile il tentativo di arruolamento, termine che la stessa Corte – come già rilevato – intende quale mero accordo; tale "serio accordo", per la Corte, è un "evento" (sic!) "altamente pericoloso". Quindi, secondo la Corte, punire chi tenta, senza riuscirvi, di accordarsi con un altro, affinché questi realizzi atti preparatori, da portare successivamente ad esecuzione, è compatibile con il principio di offensività.

ovviamente, ignorando sdegnosamente ormai obsolete questioni di dommatica e garanzie costituzionali, che si ritiene appartengano alle 'ideologie del secolo scorso'…

### *7. Cenni intorno alle misure di prevenzione antiterrorismo*

Per completare il quadro dell'eccessiva anticipazione della tutela in materia di terrorismo, occorre tener conto dell'ampliamento delle misure di prevenzione. Infatti, l'art. 4, lett. d), d.lgs. n. 159/2011, rubricato «codice delle leggi antimafia e delle misure di prevenzione» etc., come modificato da ultimo dall'art. 4, co. 1, lett. a), d.l. n. 7/2015, conv. con modif. in l. n. 43/2015, prevede l'applicabilità della sorveglianza speciale, eventualmente con divieto o obbligo di soggiorno,

> a coloro che, operanti in gruppi o isolatamente, pongano in essere atti preparatori, obiettivamente rilevanti, diretti a sovvertire l'ordinamento dello Stato, con la commissione di uno dei reati previsti dal capo I, titolo VI, del libro II del codice penale o dagli articoli 284, 285, 286, 306, 438, 439, 605 e 630 dello stesso codice nonché alla commissione dei reati con finalità di terrorismo anche internazionale ovvero a prendere parte ad un conflitto in territorio estero a sostegno di un'organizzazione che persegue le finalità terroristiche di cui all'articolo 270-*sexies* del codice penale.

Agli stessi soggetti ed ai sospetti finanziatori del terrorismo sono applicabili, in base all'art. 16 co. 1 lett. a) e b) d.lgs. n. 159/2011, anche le misure di prevenzione patrimoniali.

Inoltre, l'art. 13 co. 1 d.lgs. n. 286/1998, il t.u. in materia di immigrazione, prevede che, «per motivi di ordine pubblico o di sicurezza dello Stato», il Ministro dell'interno può disporre l'espulsione dello straniero anche non residente nel territorio dello Stato. E il co. 2 dello stesso articolo, modificato dall'art. 4 co. 2 d.l. n. 7/2015, sancisce che «l'espulsione è disposta dal prefetto, caso per caso [*sic*!], quando lo straniero: […] c) appartiene a taluna delle categorie indicate negli articoli 1, 4 e 16, del decreto legislativo 6 settembre 2011, n. 159». Tale espulsione, ai sensi dell'art. 13, co. 4 e 5 *bis*, t.u. immigrazione, è immediatamente esecutiva ed avviene mediante accompagnamento alla

frontiera a mezzo della forza pubblica, a condizione che venga convalidato entro quarantott'ore dal giudice di pace; in tal caso il provvedimento diviene esecutivo e il ricorso in Cassazione non sospende l'esecuzione.

Dunque, può applicarsi la sorveglianza speciale in rapporto alla commissione di qualunque atto preparatorio "obiettivamente rilevante" – qualunque cosa ciò significhi –, "diretto", tra altre ipotesi, alla «commissione dei reati con finalità di terrorismo anche internazionale» – quindi, ad esempio, anche un atto preparatorio rispetto agli atti… preparatori di cui agli artt. 270 *quater* e *quinquies* c.p. ed alla detenzione di precursori – «ovvero a prendere parte ad un conflitto in territorio estero a sostegno di un'organizzazione che persegue le finalità terroristiche di cui all'articolo 270-*sexies* del codice penale».

Ma tali atti preparatori legittimano anche l'espulsione prefettizia "caso per caso" e con il solo controllo, prima dell'esecuzione, del giudice di pace: si tratta sostanzialmente di postmoderne *lettres de cachet*.

Il contenuto afflittivo della sorveglianza speciale è ben noto. Si tratta di una sorta di semidetenzione domiciliare, accompagnata da alcune prescrizioni obbligatorie di spaventosa, paradigmatica indeterminatezza – prima fra tutte quella di «vivere onestamente, di rispettare le leggi» – e da tutte quelle prescrizioni facoltative che il tribunale «ravvisi necessarie, avuto riguardo alle esigenze di difesa sociale», art. 8 co. 5 d.lgs. n. 159/2011: in sostanza, una pena *ante delictum* dai contenuti gravemente indeterminati, la cui illegittimità costituzionale appare tanto evidente quanto generalmente sottaciuta.

## *8. Rilievi conclusivi. Il* trend *internazionale ed europeo e le alternative proponibili dalla cultura penalistica*

La legislazione penale italiana si inserisce – con alcune inquietanti peculiarità – in un *trend* internazionale ed europeo, quello del contrasto al terrorismo inteso in modo bellicistico, ovvero quale *war on terrorism* portata avanti con strumenti militari e con norme penali eccezionali.

In posizione servente rispetto a quella che è un'opzione politico-criminale si pone la descrizione del male da combattere, *rectius*, del nemi-

co, le cui inquietanti dimensioni planetarie e 'del tutto nuove' vengono esaltate in modo da legittimare risposte belliche e repressive durissime e del tutto nuove, non convenzionali, da cosiddetta guerra 'sporca'. Se, ad esempio, si definiscono i terroristi come soggetti nuovi, né criminali né belligeranti, ma "combattenti illegali", li si priva, com'è avvenuto a Guantanamo, sia delle garanzie del diritto penale che di quelle del diritto internazionale dei conflitti armati. Diventano "non persone". Ma una descrizione inquietante del nuovo fenomeno terroristico da 'combattere' – ad es. l'uso di *internet*, i terroristi *home grown*, i terroristi isolati – si trova all'inizio dei *considerando* e delle relazioni che accompagnano ogni normativa in materia, e talvolta anche degli studi dottrinali sul tema. Di fronte alla 'novità' del fenomeno, viene considerato ormai 'obsoleto' il riferimento a principi, garanzie e categorie dommatico-sistematiche del cosiddetto diritto penale 'classico'.

Beninteso, non si vuol negare la lesività dei fatti di terrorismo, nella misura in cui offendono beni fondamentali di una o più persone. Si vuole, invece, richiamare la necessità di evitare reazioni emotive ed irrazionali, indiscriminate e sproporzionate, che potrebbero risultare inutili o, peggio, controproducenti, e di predisporre un sistema di contrasto del terrorismo che sia conforme ai principi della cultura penalistica europea.

Sotto tale profilo, la normativa europea antiterrorismo, che vincola gli Stati anche sul piano dell'intervento penale, risulta carente da diversi punti di vista ed è sicuramente corresponsabile dell'indeterminatezza e dell'anticipazione della tutela penale che caratterizzano le norme nazionali[44]. In proposito, bisogna tener fermo, infatti, che allorché una decisione-quadro – fonte normativa che, sia pure non più prevista dopo il Trattato di Lisbona, continua a produrre i suoi effetti se emanata in precedenza – o una direttiva dell'Unione o una Convenzione del Consiglio d'Europa pongono obblighi di tutela penale, essi non consentono agli Stati una tutela penale più ristretta: cosicché, se la norma europea è indeterminata o anticipa la tutela, gli Stati non possono circoscrivere

[44] Sul punto, cfr. spec. la puntuale critica di T. WEIGEND, *The Universal Terrorist*, cit., 927 ss.; v. inoltre F. FASANI, *Terrorismo islamico e diritto penale*, cit., 140 ss.; V. MASARONE, *Politica criminale e diritto penale nel contrasto al terrorismo internazionale*, cit., 140 ss.

ulteriormente la punibilità. Il legislatore viene così sottoposto ad un vincolo che può risultare, se non proprio frontalmente in contrasto, quantomeno in forte tensione con i principi costituzionali, specialmente con quelli non comuni agli Stati europei e, in particolare, anche e soprattutto con quelli non espressamente previsti, ma ricavabili implicitamente, anche mediante un'interpretazione sistematica della Costituzione: ad esempio, i principi di determinatezza e di offensività.

Ebbene, una corresponsabilità della normativa europea antiterrorismo nell'espansione della disciplina nazionale sussiste già in considerazione dell'avallo fornito dalle istituzioni europee a norme penali indeterminate che incriminano il mero accordo, come l'art. 270 *bis* c.p.: l'art. 2, co. 1 e 2 lett. b), della decisione-quadro del 13 giugno 2002, 2002/475/GAI, definisce i concetti di organizzazione terroristica e di partecipazione alla stessa in modo alquanto indeterminato: ai sensi del co. 1, organizzazione terroristica è un'associazione "strutturata" di più di due persone, ma per associazione strutturata si intende espressamente anche un'associazione che non preveda "una struttura articolata"[45]. E ai sensi del co. 2, lett. b), la partecipazione «alle attività di un'organizzazione» si realizza "anche" fornendo informazioni o mezzi materiali o finanziandola: ma il termine "anche" pare indicare che si possa partecipare in qualsiasi altro modo.

Ma la corresponsabilità delle istituzioni europee va ben al di là della conservazione di norme di legge di problematica legittimità costituzionale: essa consiste principalmente nell'ampliamento della tutela penale, in contrasto innanzitutto con i principi di determinatezza ed offensività.

Così, la definizione di terrorismo introdotta in Italia nel 2005 all'art. 270 *sexies* c.p., su cui ci siamo già soffermati, corrisponde a quella imposta dall'art. 1 della decisione-quadro del 2002; anche se vi è una significativa differenza, consistente – come già ricordato – nel dato per cui la decisione-quadro limita le condotte terroristiche ai soli atti inten-

[45] In proposito, sia consentito rinviare al nostro *L'influenza sull'ordinamento italiano del diritto penale europeo delle organizzazioni criminali*, in A. CASTALDO, V. DE FRANCESCO, M. DEL TUFO, S. MANACORDA, L. MONACO (a cura di), *Scritti in onore di Alfonso M. Stile*, Napoli, 2013, 1259.

zionali compresi in un elenco, nel quale, peraltro, sono accomunati fatti molto diversi e finanche la semplice minaccia di commetterli[46].

Anche le norme incriminatrici italiane in tema di reclutamento ed addestramento sono state introdotte in attuazione di obblighi di tutela penale previsti dalla Convenzione del Consiglio d'Europa del 16 maggio 2005[47]. L'art. 5 della Convenzione impone agli Stati di prevedere il reato di «pubblica provocazione a commettere un reato di terrorismo», sostanzialmente riconducibile alla pubblica istigazione; ma l'art. 6 della Convenzione stessa vincola a punire il "reclutamento", definito quale istigazione o, più ampiamente, quale mera sollecitazione (il tenore letterale della norma è "to solicit") privata a commettere atti di terrorismo, punibile anche se non accolta. L'art. 7, a sua volta, vincola gli Stati a punire l'addestramento, inteso quale mero «fornire istruzioni» anche in rapporto a «specifici metodi o tecniche» per la commissione di atti terroristici. L'art. 8 precisa che le condotte di cui agli artt. da 5 a 7 devono essere punite anche se non è stato commesso alcun atto di terrorismo. A questo punto, appare evidente come l'indeterminatezza e l'anticipazione della tutela caratteristiche della normativa italiana e già sottoposte a critica riproducano vizi d'origine presenti nella disciplina europea.

La decisione-quadro 2008/919/GAI, che modifica quella del 2002, traduce in diritto dell'Unione europea gli obblighi posti dalla Convenzione del Consiglio d'Europa. L'art. 1 co. 1 modifica l'art. 3 della decisione-quadro del 2002 definendo alla lett. b) – nella versione in lingua italiana – il reclutamento quale mera "induzione" a commettere atti di terrorismo; la lett. c) riproduce la definizione di addestramento contenuta nella Convenzione. L'art. 1 co. 3 riproduce l'art. 8 della Convenzione, escludendo la necessità della commissione di alcun atto di terro-

[46] Per una condivisibile critica al riguardo, v. ancora T. WEIGEND, *The Universal Terrorist*, cit., 929-930.

[47] Sull'influenza di tale Convenzione e della decisione-quadro del 2008 negli ordinamenti tedesco, inglese e spagnolo, cfr. l'approfondita indagine comparatistica di A. PETZSCHE, *Strafrecht und Terrorismusbekämpfung. Eine vergleichende Untersuchung der Bekämpfung terroristischer Vorbereitungshandlungen in Deutschland, Großbritannien und Spanien*, Baden-Baden, 2013, 28 ss., 59 ss. e *passim*; sull'influenza delle stesse fonti sugli ordinamenti degli stati nordici, v. criticamente E.J. HUSABØ, *Die Kriminalisierung von terroristischen Straftaten und deren Vorbereitung in den nordischen Ländern*, cit., 1155 ss.

rismo ai fini della punibilità di provocazione, reclutamento e addestramento.

A fronte di un tale stato di cose, la posizione di una cospicua parte della dottrina, che, in vari Paesi europei, critica l'indeterminatezza e l'anticipazione della tutela della normativa antiterrorismo e, più in generale, la politica dominante, sul piano europeo ed internazionale, in materia, viene etichettata, in maniera strumentale, come 'vecchia'. Ciò, in particolare, sotto due profili.

Da un primo angolo visuale, si sostiene che invocare i principi costituzionali di un singolo Paese di fronte alla lotta globale al terrorismo ed all'integrazione europea non sia più possibile: entrambe, infatti, esigono, se non un'unificazione, quantomeno un'armonizzazione ed una coerenza che dovrebbe prevalere sulle peculiarità nazionali, di cui fanno parte – questo è il problema – anche quei principi costituzionali non "comuni" a tutti o alla maggior parte dei Paesi membri. Appare emblematico come lo stesso *Manifesto per una politica criminale europea* – per molti versi condivisibile –, redatto da esperti di diritto penale europeo di diversi Paesi, neghi cittadinanza ai principi costituzionali di un singolo Paese e consideri metodologicamente scorretto, da parte degli studiosi, valutare la normativa penale dell'Unione alla stregua di quei principi[48].

In tal modo, le Costituzioni nazionali e le loro garanzie fondamentali rischiano di soccombere rispetto ad una normativa penale europea che – nella più benevola, e a mio avviso non condivisibile interpretazione – si approssima, attraverso il procedimento di codecisione, ad una *lex parlamentaria*, che non ha certo rango costituzionale! E soprattutto, ciò che si profila – ed i segnali, al riguardo, sono tanti – è un inaccettabile livellamento verso il basso delle garanzie costituzionali, conservandone solo il minimo condiviso da tutti. Il principio di legalità *sub specie* riserva di legge, il principio di precisione o determinatezza della legge e non del diritto anche giurisprudenziale, il principio di personali-

[48] Cfr. P. ASP ET AL., *European criminal policy initiative. Manifesto sulla politica criminale europea*, cit., 1281. Per una critica strutturalmente simile a quella da me svolta, ma rivolta, a suo tempo, al cosiddetto *Corpus juris* europeo, cfr. A. BARATTA, *Il* Corpus juris *e la cultura giuridico-penale europea*, in AA.VV., *Ambito e prospettive di uno spazio giuridico-penale europeo*, a cura di S. MOCCIA, Napoli, 2004, 33-34.

tà della responsabilità penale, il principio di offensività, sono peculiarità di alcune Costituzioni nazionali: devono forse, in quanto tali, essere abbandonati nel contrasto del terrorismo e nel diritto penale europeo in generale?

Il secondo profilo della ritenuta 'vetustà' della cultura penalistica dei principi consiste nella riflessione – che comincia quantomeno con gli ultimi paragrafi del capolavoro di Beccaria[49]– sul retroterra politico, economico, sociale in cui si alimentano i fenomeni criminali.

Secondo l'orientamento in atto dominante nella 'lotta' al terrorismo, non vi sono concause del fenomeno su cui intervenire; vi sono solo individui e gruppi 'nemici' da combattere. Ed invece, anche in rapporto al terrorismo internazionale di matrice fondamentalista islamica, è necessario riflettere in una prospettiva di interdisciplinarità esterna e di analisi – e risposta – multifattoriale e multiagenziale, secondo l'insegnamento di Sandro Baratta[50].

Non è questa la sede per una tale ampia riflessione. Ma, sul piano politico, si dovrà partire dalla consapevolezza del dato per cui sono ormai note le responsabilità iniziali, a carico di Stati occidentali, nel sostegno e nel finanziamento pluriennale di organizzazioni fondamentaliste in Afghanistan[51]; così come sono evidenti gli effetti criminogeni della guerra in Afghanistan e della c.d. guerra preventiva in Iraq[52], mo-

[49] *Dei delitti e delle pene* (1764), ed. a cura di A. BURGIO, Milano, 1991, § XLI ss.

[50] A. BARATTA, *La politica criminale e il diritto penale della Costituzione. Nuove riflessioni sul modello integrato delle scienze penali*, in S. CANESTRARI (a cura di), AA.VV., *Il diritto penale alla svolta di fine millennio*, Torino, 1998, 24 ss.; per spunti analoghi ed ulteriori, condivisibili rilievi cfr. M. DONINI, *Il volto attuale dell'illecito penale. La democrazia penale tra differenziazione e sussidiarietà*, Milano, 2004, 85 ss., 281 ss.

[51] Sul punto, ed in particolare sulle origini di Al Quaeda, cfr. ad es. N. CHOMSKY, *11 settembre dieci anni dopo*, Milano, 2011, 17; F. FASANI, *Terrorismo islamico e diritto penale*, cit., 36-37; A. PETZSCHE, *Strafrecht und Terrorismusbekämpfung*, cit., 40-41.

[52] N. CHOMSKY, *11 settembre dieci anni dopo*, cit., XXVI e 16, ove l'Autore, purtroppo inascoltato, pochi giorni dopo gli attentati dell'11 settembre 2001 affermava: «Chiunque con una qualche conoscenza della regione si rende conto che un massiccio attacco contro la popolazione musulmana esaudirebbe le preghiere di Bin Laden e dei suoi complici e porterebbe gli Stati Uniti dentro a quella che il ministro degli Esteri francese ha definito una "diabolica trappola"». V. anche *ivi*, 73: «Un attacco contro l'Afghanistan ucciderà probabilmente un gran numero di civili innocenti, forse un nu-

tivata sulla base di prove false ed intrapresa in violazione del diritto internazionale, e delle occupazioni militari di territori da parte di Stati o coalizioni occidentali. Sono altrettanto noti il sostegno fornito da potenze mondiali a regimi autoritari[53], ad esempio in Arabia Saudita, e la tattica bellicistica di affrontare conflitti armati dagli effetti tragici sulla vita delle persone – come quello siriano, ma non solo – intervenendo direttamente con massicci bombardamenti[54] o sostenendo taluno dei contendenti, fino al silenzio assordante sui crimini di Stato contro l'umanità commessi, oppure addestrando e/o armando una delle parti in conflitto.

Ovviamente, nulla di tutto ciò giustifica il terrorismo fondamentalista: ma la costatazione degli effetti disastrosi e criminogeni delle politiche bellicistiche e del persistere della minaccia terroristica dovrebbe indurre ad una drastica revisione delle politiche estere degli Stati occidentali, che, anziché tendere alla radicalizzazione dei conflitti, miri finalmente a contribuire – principalmente attraverso vie diplomatiche e, in ipotesi di emergenza, mediante interventi esclusivamente umanitari – a porre le condizioni per processi di pacificazione, democratizzazione, emancipazione e giustizia sociale in quei territori.

In molti Paesi, in particolare africani, infestati dal terrorismo, occorrerebbe abbandonare una politica neocoloniale che sfrutta sottocosto le altrui risorse naturali ed umane ed invade mercati, in particolare vendendovi armi; salvo poi intervenire, quando troppi diseredati fuggono dalla miseria e dai conflitti armati in cui li si è fatti precipitare, e concludere accordi con cui si pagano gli Stati di provenienza perché trattengano i migranti, non importa con quali metodi. In luogo di ciò, occorrerebbe contrastare le diseguaglianze con seri piani di sviluppo economico-sociale.

In Europa, anziché erigere barriere normative e materiali e portare avanti politiche di esclusione sociale e culturale – fino all'estremo di proibire innocue forme di manifestazione di identità religiosa –, si dovrebbe agire fortemente sull'integrazione politica, sociale, economica e

---

mero enorme, in un Paese in cui milioni di persone stanno già per morire di fame. L'uccisione gratuita di civili innocenti è terrorismo, non guerra al terrorismo».

[53] Cfr. ad es. N. CHOMSKY, *11 settembre dieci anni dopo*, cit., 13, 42-43.

[54] V. ancora N. CHOMSKY, *11 settembre dieci anni dopo*, cit., 41 ss.

culturale dei soggetti marginali e dei migranti, con coraggiose riforme in tema di cittadinanza, servizi sociali, disciplina degli accessi all'immigrazione regolare: sono queste le vere 'misure di prevenzione' primaria da adottare per contrastare il terrorismo.

Sicuramente si tratta di interventi complessi, di grandi dimensioni e destinati a dare effetti nel medio e lungo periodo: ma sono convinto che essi costituiscano una risposta da attivare immediatamente, non solo perché giusta sul piano della tutela dei diritti umani, dell'eguaglianza e della pace – il che la rende improcrastinabile in sé –, ma anche perché è l'unica che possa avere prospettive di efficacia nel contrasto del terrorismo, ponendo le condizioni per sottrarre ad esso le sue risorse umane – ossia, il suo bacino di consenso e soprattutto quell'esercito di riserva dei marginali e dei diseredati, suggestionabili dal fanatismo terroristico, visto quale unica dimensione di riscatto personale[55] – ed anche quelle finanziarie: ed il riferimento è, stavolta, a quegli interventi politici, economici e diplomatici possibili nei confronti di quegli stati e di quelle organizzazioni che finanziano il terrorismo. D'altro canto, certamente l'attuale risposta prevalentemente bellicistica, con i suoi enormi costi umani, è risultata tutt'altro che efficace e va, quindi, abbandonata.

Sul piano degli interventi sanzionatori, è sicuramente necessario l'impiego del diritto penale: ma esso deve porsi come *extrema ratio*, in particolare pure rispetto ad illeciti amministrativi che siano sostanzialmente tali, al di fuori di qualsiasi truffa delle etichette. Andrebbe, quindi, radicalmente riveduta la normativa in materia di misure di prevenzione. Sanzioni amministrative di tipo ablativo possono essere valorizzate, ad esempio, in relazione a condotte di mera detenzione abusiva di cose sottoposte a regime autorizzativo. Si possono, inoltre, prevedere

[55] Sul punto, cfr. le acute considerazioni di D. TOSINI, *Terrorismo e antiterrorismo nel XXI secolo*, cit., 9 ss., 99 ss., 142 ss.; ma v. ad es. pure H.-J. ALBRECHT, *Terrorismus und Strafrecht*, cit., 20-21. Tali considerazioni sembrano valere particolarmente in rapporto all'aumento dei cosiddetti terroristi *home-grown* ed a coloro tra essi che, dopo un cosiddetto processo di radicalizzazione, agiscono solitariamente, senza alcun contatto concreto con organizzazioni terroristiche; in proposito, cfr. A. PETZSCHE, *Strafrecht und Terrorismusbekämpfung*, cit., 37 ss., 45, 47 (ove si afferma che gli attentatori di Madrid e Londra avessero legami solo ideologici con organizzazioni terroristiche), 49 ss. (ove si richiamano alcuni casi di terroristi isolati perseguiti in Germania).

poteri di indagine e controlli di polizia amministrativa, purché siano vincolati a presupposti precisamente definiti e sottoposti al controllo di un giudice, secondo le garanzie previste dalla Costituzione per le libertà di cui agli artt. 13 ss. Cost. Ogni intervento sulla libertà personale e sulla dignità della persona va, invece, assoggettato alle garanzie del diritto penale, ed in tale settore sarebbe auspicabile una profonda revisione costituzionalmente orientata delle norme in materia di terrorismo.

# LE NUOVE EMERGENZE TERRORISTICHE: IL DIFFICILE RAPPORTO TRA ESIGENZE DI TUTELA E GARANZIE INDIVIDUALI

*Roberto Bartoli*

SOMMARIO: *1. Considerazioni introduttive. 2. I caratteri specifici del fenomeno terroristico internazionale. 3. Le strategie di contrasto al terrorismo internazionale. 4. La strategia della guerra al terrorismo e la dissoluzione del concetto di diritto. 5. Le strategie dello* jus in bello *del criminale e del diritto penale del nemico: l'erosione dei pilastri della nostra civiltà giuridica. 5.1. Lo* jus in bello *del criminale. 5.2. Il diritto penale del nemico. 6. La strategia "tradizionale" tra diritto penale della normalità e diritto penale dell'emergenza. 7. Considerazioni conclusive.*

## *1. Considerazioni introduttive*

Anche il terrorismo internazionale, al pari di ogni fenomeno criminoso, pone il problema della perenne tensione tra esigenze di difesa sociale ed esigenze di garanzia. Non solo, andando più a fondo, si può dire che la "lotta" al terrorismo internazionale ripropone, in termini rinnovati alla luce dei mutamenti determinati dalla modernità, la perenne tensione tra sovranità e diritti fondamentali: se, da un lato, per difendere i diritti occorre concentrare la forza nella sovranità; dall'altro lato, è indispensabile difendersi anche dalla stessa sovranità che, proprio al fine di tutelare i diritti, tende a violarli[1].

Tuttavia, a ben vedere, la lotta al terrorismo internazionale pone anche problemi assai più rilevanti, oserei dire cruciali, forse addirittura

[1] P. COSTA, voce *Diritti fondamentali (storia)*, in *Enc. dir.*, *Annali II*, tomo II, Milano, 2008, 373 s.; D. PULITANÒ, *Diritti umani e diritto penale*, in M. MECCARELLI, P. PALCHETTI, C. SOTIS (a cura di), AA.VV., *Il lato oscuro dei Diritti umani. Esigenze emancipatorie e logiche di dominio nella tutela giuridica dell'individuo*, Madrid, 2014, 87 ss.; nonché, volendo, R. BARTOLI, *"Chiaro e oscuro" dei diritti umani alla luce del processo di giurisdizionalizzazione del diritto*, *ivi*, 138 ss.

epocali. Ed infatti, mentre rispetto a tutti gli altri fenomeni criminosi si tende ad elaborare strumenti che si pongono anche in fortissima tensione con i principi e le garanzie, senza metterne però in discussione i pilastri fondamentali sui quali tali principi e tali garanzie si reggono; al contrario, nella lotta al terrorismo internazionale si tende a elaborare strumenti che pongono in discussione gli stessi pilastri su cui si reggono i principi e su cui si basa il sistema giuridico-istituzionale: starei per dire che il terrorismo internazionale pone in discussione addirittura lo stesso concetto ordinante del diritto.

In particolare, gli strumenti di lotta al terrorismo internazionale tendono a contestare alla radice una distinzione basilare, una sorta di fondamento preliminare che sta alla base degli stessi principi e limiti costituzionali: si tratta della distinzione tra diritto in tempo di pace e diritto in tempo di guerra. Per rendersi conto di questo assunto è sufficiente mettere in evidenza questi aspetti.

Da quando è (ri)sorto il problema del terrorismo internazionale, nel diritto in tempo di pace si è iniziato a parlare di criminali come nemici. Il terrorista, cioè, non sarebbe il "solito" criminale che mediante il suo comportamento realizza fatti che esprimono un certo disvalore, ma sarebbe un nemico dello Stato, perché, pur realizzando un reato, ha intenzione di spazzare via le istituzioni che governano uno Stato ed è pronto al sacrificio di sé proprio come fa un autentico combattente quando combatte una guerra.

Non solo, ma nel diritto in tempo di guerra, si è iniziato ad affermare un concetto discriminatorio di guerra e a parlare di nemici che devono essere trattati come criminali. Se un legittimo combattente appartiene a una parte del conflitto che tuttavia viene qualificata come parte "terrorista", questo combattente legittimo non può uccidere altri combattenti legittimi: se lo fa, viene considerato un criminale che deve essere processato e condannato, quando invece secondo il diritto internazionale umanitario chi è combattente legittimo e uccide nel rispetto dello *jus in bello* il suo comportamento è lecito, visto che altrimenti si rischia di scatenare una guerra senza più limiti.

Infine, ma direi soprattutto, si è iniziato a parlare della possibilità di realizzare una guerra al terrorismo, di utilizzare cioè lo strumento bellico, le armi, contro chi appartiene a un'organizzazione criminale e quin-

di nella sostanza è un criminale. In questa prospettiva, un terrorista non solo non può uccidere altri poiché altrimenti pone in essere un reato, ma addirittura, se uccide, pur essendo un criminale che deve essere processato e condannato, può essere ucciso in qualsiasi momento attraverso un'azione militare, come è accaduto a Osama bin Laden capo dell'organizzazione terroristica Al-Qaida.

Se quanto detto è vero, il tema del terrorismo internazionale diventa un tema davvero centrale, vale a dire il tema dove si gioca lo stesso destino del diritto, non soltanto con riferimento alla sua capacità di porre limiti alla forza, ma addirittura con riferimento alla sua stessa capacità di ordinare, razionalizzare, distinguere. La lotta al terrorismo ha mostrato il rischio di minare alle fondamenta il diritto, di pervertire il concetto di diritto, di confondere concetti giuridici nati per dare ordine razionale alle cose e quindi razionalità, sistema e garanzia.

## *2. I caratteri specifici del fenomeno terroristico internazionale*

Perché proprio il terrorismo internazionale ha posto queste problematiche fondamentali?

In estrema sintesi, si può affermare che il fenomeno del terrorismo internazionale presenta almeno cinque caratteri "criminosi" davvero peculiari. Anzitutto, sul piano soggettivo, si contraddistingue per una prospettiva assolutamente nemicale. Il terrorista, come accennato, non si pone infatti come un mero criminale che anche là dove contraddice valori significativi della convivenza si limita a "contestarli" in termini – per così dire – negativi, mantenendo pur sempre un rapporto di fondo con la società in cui è inserito; il terrorista è piuttosto un portatore di valori fondamentali alternativi che vuole sostituire a quelli contro i quali "combatte".

In secondo luogo, sul piano oggettivo, il terrorista agisce strumentalizzando soggetti che risultano "innocenti", vale a dire estranei rispetto allo stesso conflitto che ha ingaggiato. Se originariamente il disvalore del terrorismo veniva individuato nella sua capacità di perseguire obiettivi politici mediante l'impiego della violenza, oggi il disvalore si incentra soprattutto nell'arrecare offesa immediata e diretta a persone che

nulla hanno a che vedere con il conflitto. In sostanza, si vuole abbattere un sistema, ma per abbatterlo non si prende di mira direttamente chi è al vertice governativo di quel sistema, ma piuttosto si offendono soggetti che risultano in definitiva estranei alle responsabilità di guida dello stesso. E nell'offesa di un terzo innocente – per così dire – totalmente estraneo al conflitto si concretizza una totale indifferenza nei confronti dell'identità personale della vittima e una strumentalizzazione della sua persona ad altri fini, aspetti che finiscono per mettere in gioco lo stesso concetto di dignità umana.

In terzo luogo, sempre sul piano oggettivo, il terrorismo internazionale si concretizza per un'offensività "variabile", in quanto si può andare da comportamenti offensivi davvero minimi, per non dire simbolici, fino a comportamenti con una carica offensiva intensissima che per l'appunto si approssima a un vero e proprio atto bellico.

Ed ancora, sul piano modale, l'attività terroristica presuppone l'esistenza di una organizzazione che si caratterizza per una sua extraterritorialità. In particolare, da un lato, proprio il perseguimento reale di una finalità come il sovvertimento di un sistema, postula un'organizzazione di più soggetti, potendosi affermare che deve esistere una sorta di corrispondenza tra la consistenza dell'obiettivo che si persegue e la consistenza dell'organizzazione, per cui più il primo ha una vasta portata, più la seconda deve possedere una struttura organizzativa idonea. Dall'altro lato, il terrorismo internazionale comporta che il nucleo centrale dell'organizzazione si trovi collocato fuori dallo Stato in cui si pongono in essere le azioni terroristiche o comunque comporta che l'organizzazione si frammenti in più territori divenendo difficile la stessa localizzazione del nucleo centrale.

Infine, sempre sul piano modale, anche alla luce dei più recenti attacchi realizzati in Europa, si deve considerare che un'attività terroristica può essere realizzata anche da parte di uno Stato o direttamente (attraverso le proprie forze armate oppure avvalendosi di soggetti esecutori che agiscono sotto il controllo diretto dello Stato mandante) oppure avvalendosi di organizzazioni terroristiche internazionali, potendosi distinguere tra l'ipotesi in cui l'attentato terroristico assume i connotati di un vero e proprio attacco alla sovranità territoriale del paese nemico

e l'ipotesi in cui invece l'atto terroristico non riesce a superare la soglia del conflitto armato esprimendo nella sostanza un disvalore criminale.

Ebbene, è alla luce di questi caratteri che mi pare si possa comprendere la ragione per cui la lotta al terrorismo si presta ad elaborare strumenti che "confondono" la dimensione bellica e quella criminale. Se infatti si valorizza la dimensione soggettiva, la prospettiva che si adotta nella configurazione dei mezzi di risposta non può che essere bellica. Se invece si valorizza la dimensione oggettiva, la prospettiva muta a seconda delle modalità di manifestarsi del terrorismo, per cui se il terrorismo si manifesta particolarmente offensivo (forte strumentalizzazione delle vittime, attentati su larga scala, extraterritorialità), si è indotti ad assumere una prospettiva bellica, mentre se la gravità risulta attenuata (scarsa strumentalizzazione delle vittime, attentati su scala ridotta, intraterritorialità), la prospettiva non può che essere criminale. Inoltre, nel momento in cui l'attività terroristica è riconducibile a uno Stato, va da sé che si aprano ancora di più i margini per una prospettiva autenticamente bellica.

## *3. Le strategie di contrasto al terrorismo internazionale*

Nella lotta al terrorismo internazionale sono state elaborate tre diverse strategie: quella della guerra al terrorismo, quella del diritto penale del nemico e dello *jus in bello* del criminale e infine la strategia "tradizionale" che distingue tra diritto in tempo di guerra e diritto in tempo di pace e all'interno di quest'ultimo tra un diritto penale della normalità e un diritto penale dell'emergenza.

## *4. La strategia della guerra al terrorismo e la dissoluzione del concetto di diritto*

La strategia della guerra al terrorismo è stata elaborata negli Stati Uniti d'America, dove cioè si è avuta la manifestazione più cruenta del terrorismo. Tale strategia si basa sulla valorizzazione della componente soggettiva del fenomeno terroristico. Ancora più a fondo, si può dire

che in questa prospettiva l'attacco terroristico è considerato di una gravità assoluta, per certi aspetti più grave dello stesso attacco bellico, perché, in virtù della sua inefficacia rispetto allo scopo, in virtù della sua offesa esclusiva a civili innocenti estranei al conflitto, rappresenta una sorta di male fine a se stesso, una mera crudeltà inumana. Da qui una assolutizzazione, una astrazione, una unificazione dei concetti, per cui si tende a superare la distinzione tra tempo di pace e tempo di guerra e a introdurre il *tertium genus* della "guerra al terrorismo".

Rilevantissime le conseguenze sul piano della "disciplina", sia sul piano internazionale che del diritto interno. Sul piano internazionale, anzitutto, si hanno conseguenze in ordine allo *jus ad bellum*, al diritto, cioè, che disciplina l'uso della forza: non solo si ritiene legittimo l'uso della forza preventiva, vale a dire l'uso della forza a prescindere dalla sussistenza dei presupposti che legittimano una difesa armata, ma addirittura, e questa è la vera e propria novità, si ritiene che si possa ingaggiare una vera e propria guerra contro una mera organizzazione criminale.

In secondo luogo, sempre sul piano internazionale, vi sono conseguenze in ordine allo *jus in bello*, al diritto, cioè, che disciplina le modalità di conduzione del conflitto: rispetto a questo diritto si assiste all'eliminazione della distinzione fondamentale tra combattente legittimo e civile e all'introduzione di una terza categoria, quella del combattente illegittimo, rispetto al quale non trovano applicazione le Convenzioni di Ginevra e i Protocolli Aggiuntivi, con la conseguenza che il combattente illegittimo non è né un nemico, né un criminale. In particolare, da un lato, il combattente illegittimo non può uccidere il combattente nemico, ma può essere ucciso in qualsiasi momento: effetto ultimo di questa strategia sono gli omicidi mirati e l'impiego della forza armata in contesti di pace. Dall'altro lato, se catturato, proprio perché non è combattente, il combattente illegittimo deve essere detenuto, ma non processato, perché non è nemmeno un civile-criminale. La detenzione del combattente illegittimo non conosce quindi limiti, né spaziali, né temporali, perché la guerra al terrorismo è una guerra che non conosce limiti.

Sul piano del diritto interno, si va verso la proclamazione di uno stato d'emergenza (più opportuno parlare di un vero e proprio stato di ec-

cezione) assoluto: sul piano istituzionale, si concentrano tutti i poteri nelle mani dell'esecutivo; sul piano delle garanzie, esse vengono interamente sospese comprese quelle davvero fondamentali aventi carattere giurisdizionale.

In sostanza, il combattente illegittimo non è né un nemico, né un criminale, ma un nemico assoluto dell'intera umanità, vale a dire un uomo degradato a non-persona. Ecco cosa è stata la realtà di Guantanamo: uno strumento di annientamento del nemico assoluto.

## *5. Le strategie dello* jus in bello *del criminale e del diritto penale del nemico: l'erosione dei pilastri della nostra civiltà giuridica*

Si tratta di due strategie sorte in contesti in cui la lotta terroristica non è divenuta particolarmente cruenta, e più precisamente all'interno della nostra Europa a seguito dei primi attacchi realizzati a partire dal 2005. Se, da un lato, siffatte strategie, rispetto alla distinzione tra diritto in tempo di pace e diritto in tempo di guerra, non giungono ad esiti di rottura così eclatanti, come nel caso della strategia della guerra al terrorismo, dall'altro lato, però, sia all'interno del diritto in tempo di guerra che di quello in tempo di pace danno luogo a forzature assai significative che erodono i pilastri fondanti della nostra civiltà giuridica.

### *5.1. Lo* jus in bello *del criminale*

In particolare, lo strumento dello *jus in bello* del criminale si caratterizza per il fatto che, all'interno del diritto in tempo di guerra, viene compiuta una discriminazione tra i combattenti legittimi appartenenti alle due parti avverse che partecipano ad un conflitto armato, per cui gli atti compiuti nel rispetto dello *jus in bello*, se realizzati da combattenti legittimi appartenenti ad una parte, sono considerati leciti, mentre se realizzati dall'altra parte (sempre nel rispetto dello *jus in bello*) sono tuttavia considerati crimini e più precisamente atti terroristici.

Un'espressione di questa strategia si è avuta nel nostro ordinamento a seguito della formazione di un orientamento giurisprudenziale che, attraverso una progressiva estensione del concetto di atto terroristico,

ha considerato punibili per terrorismo internazionale soggetti che, in quanto meri combattenti legittimi, avevano tuttavia realizzato atti conformi allo *jus in bello*.

In particolare, in un primo momento, si è considerato terroristico l'attacco di combattenti legittimi che aveva come destinatari combattenti legittimi ed anche civili per il solo fatto che erano stati offesi anche soggetti civili, quando invece per il diritto umanitario un attacco di combattenti legittimi contro combattenti legittimi che colpisca anche civili è terroristico soltanto se esiste una sproporzione tra l'obiettivo militare che si perseguiva e le vittime civili.

Ed infatti, nel 2007 la Corte di Cassazione, dato per scontato che costituiva terrorismo l'atto bellico realizzato a danno esclusivo della popolazione civile, e che, per converso, si consideravano leciti gli atti conformi allo *jus in bello* posti in essere da combattenti legittimi nei confronti di altri combattenti legittimi, fossero essi impegnati o meno direttamente in operazioni militari, ha precisato quanto segue:

> nei contesti di conflitto armato possono ben presentarsi situazioni nelle quali gli atti di violenza sono rivolti contro militari quanto contro la popolazione civile, allorquando – per la natura di tali atti, per i mezzi impiegati e per le specifiche condizioni nelle quali sono compiuti – risultano sicuramente produttivi di gravi danni non solo militari ma anche civili[2]

con la conseguenza che

> costituisce atto terroristico anche quello contro obiettivo militare quando le peculiari e concrete situazioni fattuali facciano apparire certe ed inevitabili le gravi conseguenze in danno della vita e dell'incolumità fisica della popolazione civile, contribuendo a diffondere nella collettività paura e panico[3].

In buona sostanza, all'interno del contesto bellico, la Corte ha distinto due diversi atti di terrorismo, quello compiuto a danno esclusivo dei

[2] Cfr. Cass. pen., Sez. I, 11 ottobre 2006-17 gennaio 2007, Bouyahia Maher, in *Guida dir*., 2007, n. 17, 90 ss.

[3] Cfr. Cass. pen., Sez. I, 11 ottobre 2006-17 gennaio 2007, Bouyahia Maher, cit., 98.

civili e quello, invece, "misto", diretto contro militari, con conseguenze anche per i civili, rispetto al quale occorrono requisiti aggiuntivi, e cioè sul piano oggettivo, danni gravi; sul piano soggettivo, una sorta di dolo diretto.

Tuttavia, tale nozione di atto terroristico suscita perplessità nella parte relativa agli attacchi "misti". Ed infatti, non c'è dubbio che sul piano oggettivo un attacco terroristico può sussistere anche quando è diretto verso militari. Ma poiché si tratta di un attacco che ha come oggetto per l'appunto anche militari, se sul piano soggettivo è corretto richiedere la certezza (il dolo diretto) che tale attacco causerà offese anche alla popolazione civile, ciò che determina disvalore oggettivo non è, come ha ritenuto la Corte, la gravità delle offese in sé e per sé considerate, bensì, la realizzazione di offese eccessive e sproporzionate rispetto al vantaggio militare concreto previsto. Ed infatti, da un punto di vista meramente formale, le stesse Convenzioni internazionali considerano illegittimo l'attacco indiscriminato che colpisce la popolazione civile o i beni di carattere civile in termini eccessivi rispetto agli obiettivi militari (art. 85, par. 3, lett. b), in combinazione con l'art. 57, par. 2, lett. a), iii), I PACG). Da un punto di vista sostanziale, poi, il carattere sproporzionato e il dolo diretto sono richiesti proprio perché nella situazione del conflitto bellico, in cui uccidere (purtroppo, ma inevitabilmente) costituisce la regola, soltanto il danno sproporzionato e la certezza sono in grado di esprimere un disvalore tale da renderlo punibile.

Non solo, ma in un secondo momento la nozione di attacco terroristico in contesto di conflitto armato con esiti discriminatori è stata ulteriormente estesa. Sulla scia di due arresti precedenti[4], la Corte di Cassazione ha affermato che il terrorismo internazionale

> si connota, anche se posto in essere in tempo di guerra, per la identità delle vittime (che debbono essere civili o soggetti comunque non impegnati nelle operazioni belliche), per la motivazione politica, religiosa o ideologica (secondo una norma consuetudinaria internazionale accolta

[4] Cass. pen., Sez. V, 4 luglio 2008-22 ottobre 2008, Ciise Maxamed, in *CED Cass*., n. 39545/2008; Cass. pen., Sez. V, 18 luglio 2008-7 gennaio 2009, Laagoub Abdelkader, *ivi*, n. 75/2009.

> in varie risoluzioni dall'assemblea generale dell'Onu) e, infine, da quel dato intrinseco alla nozione di terrorismo che è costituito dall'anonimato delle persone colpite dalle azioni violente, come si deve arguire dal rilievo che deve trattarsi della finalità di seminare indiscriminata paura nella collettività[5].

Dal concetto di terrorismo internazionale in tempo di guerra sarebbero quindi esclusi «solo comportamenti volti a colpire un obiettivo militare, quando comunque sia assente la finalità di intimidire la popolazione o di costringere il governo a un atto diverso da quello che avrebbe compiuto»[6]. Ed ancora:

> nel senso qui accolto, si è espressa, come detto, anche la sentenza di questa Corte del 2006 – emessa in relazione al fenomeno del reclutamento e all'invio di volontari del fondamentalismo islamico in campi di assestamento […] – la quale ha condivisibilmente escluso dalla finalità di terrorismo internazionale, le sole azioni poste in essere anche da formazioni clandestine dirette esclusivamente contro combattenti, che restano soggette alla disciplina del diritto internazionale umanitario, mentre nel caso di atti terroristici destinati contro civili o contro persone non impegnate attivamente nelle ostilità, con il movente e le finalità sopra dette, a prescindere dalla qualità soggettiva dell'agente, la stessa sentenza ha ritenuto non disapplicabile la normativa di diritto comune, per la inesistenza di incompatibilità fra terrorismo e situazioni di conflitto armato[7].

Ebbene, la Corte sembra escludere dalla nozione di terrorismo soltanto l'atto realizzato contro militari che partecipano direttamente alle operazioni di guerra, mentre tutti gli altri atti sembrano integrare gli estremi del terrorismo internazionale: non solo gli atti esclusivamente contro i civili, e quelli "misti" contro militari e civili, ma anche addirittura gli atti contro militari non impegnati direttamente nel conflitto bellico.

---

[5] Cass. pen., Sez. V, 22 novembre 2013-21 gennaio 2014, Legori, in *Giur. it*., 2014, 1724 ss., con nota di R. BARTOLI, *Ancora equivoci in tema di terrorismo internazionale nei contesti di conflitto armato*, *ivi*, 2014, 1728 ss.

[6] Cass. pen., Sez. V, 22 novembre 2013-21 gennaio 2014, Legori, cit.

[7] Cass. pen., Sez. V, 22 novembre 2013-21 gennaio 2014, Legori, cit.

Due gli aspetti centrali che meritano di essere messi in evidenza. Il primo è che lo strumento per realizzare siffatta discriminazione è stata la nozione di terrorismo, nel senso che per la giurisprudenza tale nozione è unitaria, valida cioè sia per il tempo di pace che per il tempo di guerra, e si ricava dalla Convenzione ONU di New York del 1999, la quale ai sensi dell'art. 2, comma 1, lett. b), Convenzione O.N.U., stabilisce che

> commette un reato ai sensi della presente Convenzione chiunque con qualsiasi mezzo […] fornisce o raccoglie fondi […] al fine di compiere […] qualsiasi altro atto diretto a causare la morte o gravi lesioni fisiche ad un civile, *o a qualsiasi altra persona che non è parte attiva in situazioni di conflitto armato*, quando la finalità di tale atto, per la sua natura o contesto, è di intimidire una popolazione, o obbligare un governo o un'organizzazione internazionale a compiere o a astenersi dal compiere qualcosa[8].

Tuttavia, utilizzare tale nozione di terrorismo nei contesti bellici suscita notevoli perplessità, perché, secondo il diritto internazionale umanitario, un atto contro militari, anche se non partecipano direttamente al conflitto, è addirittura un atto lecito, se realizzato da combattenti legittimi nel rispetto dello *jus in bello*.

Secondo punto. La posizione assunta dalla Corte di Cassazione, oltre all'adozione di una nozione di terrorismo che risulta disfunzionale al contesto bellico, comporta una conseguenza ulteriore, assai più dirompente, e cioè la discriminazione tra legittimi combattenti. Ed infatti, nel momento in cui la Corte afferma che ad una parte si applica la Convenzione O.N.U. del 1999 con la relativa nozione latissima di terrorismo internazionale, afferma anche implicitamente che ai combattenti dell'altra parte si applica invece il diritto internazionale umanitario. Ma la

[8] A sostegno della soluzione prospettata dalla giurisprudenza cfr. A. VALSECCHI, *La definizione di terrorismo dopo l'introduzione del nuovo art. 270* sexies *c.p.*, in *Riv. it. dir. proc. pen*., 2006, 1113 ss.; ID., *Sulla definizione di terrorismo "in tempo di guerra"*, in *Dir. pen. contemp*., 2012, 191 ss.; L.D. CERQUA, *Sulla definizione di terrorismo internazionale*, in *Cass. pen*., 2007, 1580; F. VIGANÒ, *La nozione di "terrorismo" ai sensi del diritto penale*, in F. SALERNO (a cura di), AA.VV., *Sanzioni "individuali" del Consiglio di Sicurezza e garanzie processuali fondamentali*, Padova, 2010, 193 ss.

conseguenza di questa discriminazione è davvero devastante, perché è facile comprendere che fatti identici, e quindi atti bellici conformi allo *jus in bello*, finiscono per essere trattati in modo diverso. Così ad esempio, l'uccisione di un legittimo combattente non direttamente impegnato nelle operazioni di guerra, mentre costituisce un fatto lecito se realizzato dal legittimo combattente appartenente ad una parte, al contrario costituisce un fatto illecito, addirittura qualificabile come terrorismo, se realizzato da un appartenente alla parte avversa.

Ciò che sfugge alla Corte di Cassazione è che non solo il diritto internazionale umanitario adotta una nozione di terrorismo peculiare, diversa da quella che si adotta in tempo di pace, ma soprattutto, in presenza di legittimi combattenti, impone di applicare a tutte le parti del conflitto la stessa identica disciplina. La *ratio* di questo fondamentale principio di parità di trattamento tra combattenti è tanto semplice quanto gravida di implicazione, e cioè quella di limitare la guerra. Ed infatti, se tra le parti in conflitto fosse creato un dislivello, per cui rispetto a un fatto identico una parte è punita e l'altra no, la parte che verrebbe punita, poiché saprebbe che sarebbe punita anche se rispetta le regole, non avrebbe più motivo di agire in modo conforme allo *jus in bello*.

### *5.2. Il diritto penale del nemico*

La strategia del diritto penale del nemico si caratterizza per il fatto che, all'interno del diritto in tempo di pace, vengono adottati strumenti che incidono sulla libertà del soggetto, ma in assenza delle minime garanzie fondamentali.

Sul concetto di diritto penale del nemico occorre chiarirsi subito. Non penso che tale "diritto" possa essere identificato solo e semplicemente con qualsiasi disciplina penalistica che si pone in tensione con i principi di garanzia (determinatezza, sproporzione, offensività). Se così fosse, ogni legge costituzionalmente illegittima sarebbe espressione del diritto penale del nemico. Il diritto penale del nemico presenta piuttosto alcuni caratteri specifici che, come accennato, segnano una radicale rottura con il sistema delle garanzie.

In particolare, si possono delineare i seguenti caratteri. Anzitutto, l'autore viene ricondotto a una categoria di soggetti individuata in ter-

mini "nemicali". In secondo luogo, la risposta sanzionatoria si trasforma da preventiva a neutralizzante. In terzo luogo, si ha la tendenza a punire fatti che si collocano prima della stessa fase esecutiva, con conseguente violazione dei principi di materialità e personalità della responsabilità penale. Infine, e direi soprattutto, il tratto maggiormente significativo è offerto dalla degiurisdizionalizzazione, nel senso che la disciplina è congegnata in modo tale che il destinatario è nella sostanza nell'impossibilità di far valere le proprie ragioni davanti al giudice, con la conseguenza che è non solo nell'impossibilità di "difendersi", ma anche nell'impossibilità di attivare gli strumenti di garanzia costituzionalizzati che nel nostro sistema passano necessariamente dal potere giurisdizionale.

Alla luce di questi caratteri, si può affermare che nel nostro ordinamento v'è stata una sola misura espressione del diritto penale del nemico, vale a dire l'espulsione preventiva come disciplinata dall'art. 3 (in particolare, comma 2) d.l. n. 144 del 2005, conv. legge n. 155 del 2005, vigente dal luglio 2005 fino al 31 dicembre 2007, che poteva essere disposta dal Ministro dell'interno o dal Prefetto nell'ipotesi in cui «vi siano fondati motivi di ritenere che la permanenza dello straniero nel territorio dello Stato possa in qualsiasi modo agevolare organizzazioni o attività terroristiche anche internazionali». Tale espulsione, infatti, potendo essere eseguita immediatamente, era nella sostanza priva di una vera e propria garanzia giurisdizionale.

Alla stessa stregua, può essere considerato espressione di un diritto penale del nemico l'originario meccanismo del c.d. *listing*, il quale comportava l'automatico congelamento dei beni a prescindere da qualsiasi accertamento giudiziario nel momento in cui un soggetto veniva inserito all'interno della lista. Fortunatamente, però, a seguito di due sentenze della Grande Camera della Corte di giustizia delle Comunità europee e della Grande Camera della Corte europea dei diritti dell'uomo, si è affermato che anche il diritto dell'ONU deve essere conforme ai principi di garanzia europei, dovendosi garantire un controllo giurisdizionale completo ed effettivo che possa condurre ad una richiesta di

cancellazione del nominativo dalle liste oppure ad una deroga al congelamento dei beni[9].

Al netto di queste esperienze, non penso si possa parlare di diritto penale del nemico, né riguardo al diritto penale sostanziale, così come riformato nel 2005, nel 2015 e nel 2016, né riguardo alle misure di prevenzione introdotte nel 2015, anche perché viene garantita la riserva di giurisdizione. Piuttosto la recente legislazione sembra muoversi in una logica emergenziale.

## *6. La strategia "tradizionale" tra diritto penale della normalità e diritto penale dell'emergenza*

Venendo quindi alla strategia di contrasto al terrorismo "tradizionale", essa, oltre a continuare a distinguere in modo netto tra diritto in tempo di guerra e diritto in tempo di pace, all'interno di quest'ultimo compie anche una distinzione tra un diritto penale della normalità e un diritto penale dell'emergenza. Non c'è dubbio, infatti, che il terrorismo può creare una situazione peculiare capace di minare le basi della convivenza all'interno di una nazione o comunque creare un vero e proprio clima di "terrore" all'interno della società. E rispetto a una situazione del genere è altrettanto indubbio che gli strumenti ordinari tipici delle situazioni di normalità si possono rivelare inefficaci.

So bene che il concetto di emergenza fa paura, perché apre a deroghe e al rischio che strumenti che dovrebbero avere un termine diventino poi in realtà definitivi. D'altra parte, le garanzie rischiano di essere compromesse più da visioni rigide che, essendo incapaci di muovere dalla realtà, non la disciplinano, finendo così la realtà per avere il sopravvento sul diritto, che da visioni più flessibili, capaci di guardare alla realtà come essa è e di contenerla.

[9] Corte di giustizia delle Comunità europee (Grande Sezione), 3 settembre 2008, Kadi e Al Barakaat c. Consiglio dell'UE, in *Cass. pen*., 2009, 389 ss., con nota di A. BALSAMO, G. DE AMICIS, *Terrorismo internazionale, congelamento dei beni e tutela dei diritti fondamentali nell'interpretazione della Corte di giustizia*, *ivi*, 2009, 401 ss.; Corte EDU, sent. 12 settembre 2012, Nada c. Svizzera, in *www.dirittopenalecontemporaneo.it*.

Per introdurre questo concetto di emergenza voglio utilizzare le parole di Giuliano Vassalli, Maestro del diritto che non può certo essere accusato di avere una visione volta a smantellare le garanzie del nostro sistema:

> non tutto il diritto penale dell'emergenza è inquadrabile negli schemi del diritto penale del nemico. A mio avviso – prosegue Vassalli – quest'ultimo [il diritto penale del nemico] non è che una piccola parte del dritto dell'emergenza, una parte estrema, marginale, intollerabile in un diritto ispirato a regole di civiltà […] Gli altri istituti dell'emergenza rientrano negli schemi ordinari sotto il profilo di una politica criminale intelligente ed accettabile, non contrastante con la Costituzione, retta da ragionevolezza e opportunità[10].

Ciò premesso, anzitutto vediamo perché la recente legislazione di diritto penale sostanziale si muove in una logica emergenziale. Tradizionalmente, le fattispecie che sono utilizzate per contrastare il terrorismo internazionale si basano su un paradigma anticipatorio che si articola nella incriminazione degli atti preparatori e delle associazioni con finalità terroristica. La punizione degli atti preparatori ha come punto di riferimento un delitto specifico ben individuato; la fattispecie associativa incentra il disvalore sull'esistenza di un'organizzazione che persegue una duplice finalità: una finalità "finale", consistente nella intimidazione della popolazione, nella costrizione dei poteri pubblici a compiere o astenersi da compiere un qualsiasi atto e nella destabilizzazione o distruzione delle strutture politiche, costituzionali economiche e sociali di un Paese; e una finalità "strumentale", consistente in un programma di condotte violente che per loro natura o contesto possono arrecare grave danno ad un Paese (art. 270-*sexies*).

Le nuove fattispecie introdotte dal 2005 si caratterizzano, invece, per *non essere* riconducibili né all'associazione, in quanto tutte le condotte che sono punite devono porsi fuori dalla partecipazione all'associazione (tutte le nuove fattispecie contemplano la clausola di riserva "fuori dai casi di cui all'art. 270-*bis*"); né a veri e propri atti preparatori,

[10] G. VASSALLI, *I diritti fondamentali della persona alla prova dell'emergenza*, in S. MOCCIA (a cura di), AA.VV., *I diritti fondamentali della persona alla prova dell'emergenza*, Napoli, 2009, 32 s.

perché non devono essere orientate alla realizzazione di uno specifico e ben individuato fatto di reato, ma devono essere sorrette dalla duplice finalità "finale" e "strumentale" tipica della associazione terroristica (tutte le nuove fattispecie fanno riferimento alla finalità di terrorismo di cui all'art. 270-*sexies*): ciò vale per la fattispecie di arruolamento, che punisce sia l'arruolatore che l'arruolato (art. 270-*quater*); per la fattispecie di organizzazione di trasferimenti (art. 270-*quater*.1); per la fattispecie di addestramento, che punisce sia l'addestratore e l'istruttore che l'addestrato, l'istruito e l'auto-istruito (art. 270-*quinquies*); per la fattispecie di finanziamento (art. 270-*quinquies*.1). In buona sostanza, ci troviamo davanti a un nuovo paradigma anticipatorio del tutto peculiare che assembla insieme condotte preparatorie rispetto a una finalità criminosa del tutto generica.

Ebbene, come valutare queste nuove fattispecie? Dal punto di vista dell'*an*/*quomodo* della punibilità, non c'è dubbio che se si ragionasse nei termini della "normalità" si tratterebbe di fattispecie che vìolano i principi di garanzia, in particolare il principio di offensività/ragionevolezza, trattandosi di condotte troppo anticipate. Tuttavia se si ragiona in termini di "emergenza", si può ritenere che queste fattispecie abbiano una loro plausibilità, anche perché rispetto al rischio di attentati che hanno come vittime persone innocenti del tutto indeterminate per qualità e quantità, si è venuta affermando ormai, anche a livello internazionale, una logica a "rischio zero". Com'è stato efficacemente affermato ci troviamo in presenza della massima anticipazione oltre la quale non è possibile andare[11].

Vero questo, è anche vero che l'emergenza, pur basandosi su nuovi punti di equilibrio tra esigenze di garanzia ed esigenze preventive, deve risultare comunque razionale. E in questa prospettiva ci si rende conto che se alcune delle fattispecie che abbiamo menzionato possono reggere a un vaglio di costituzionalità "emergenziale", altre pongono invece problemi difficilmente risolvibili. Così, ad esempio, senza alcun dubbio la fattispecie di addestramento, pur essendo contraddistinta da un'anticipazione svincolata dalla riferibilità a uno specifico reato, può caratte-

[11] M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale al limite*, in *Gli speciali di Questione Giustizia*, settembre 2016, 99 ss.

rizzarsi per una concreta pericolosità che legittima l'intervento penale là dove ci si trovi in presenza di soggetti che abbiano effettivamente fornito o acquisito conoscenze per la realizzazione di attentati, anche perché l'addestramento impartito o acquisito finisce per essere riferibile a un attentato che non può non presentare caratteri di concretezza. Già più problematica risulta la fattispecie di arruolamento, dove tuttavia si può richiedere come correttivo che i due soggetti dell'arruolatore e dell'arruolato abbiano elaborato un programma criminoso comunque sufficiente determinato, potendosi parlare di un accordo a realizzare un fatto o fatti di reato che devono presentare un minimo di specificità. Al contrario, le fattispecie di organizzazione dei trasferimenti e di finanziamento non sembrano suscettibili di una "correzione" in termini di offensività maggiormente concreta, essendo condotte che di per sé si collocano lontanissime anche dalla realizzazione di un programma criminoso ancorché sufficientemente determinato. Parimenti risultano molto problematiche le fattispecie di istruzione e autoistruzione in quanto si tratta di condotte che di per sé costituiscono l'esercizio di un diritto.

Vero questo, è anche vero che queste fattispecie pongono comunque insuperabili problemi di legittimità per quanto riguarda il *quantum* di pena. Se infatti, si muove dall'idea che i fatti di associazione e di attentato sono più gravi dei fatti previsti dalle fattispecie in esame, ci si rende conto che queste ultime sono punite con pene sproporzionate ed irragionevoli. Così, l'arruolatore e il finanziatore sono puniti come chi ricopre un ruolo di vertice in una associazione (reclusione da 7 a 15 anni); l'arruolato e l'organizzatore di trasferimenti sono puniti nel minimo come il partecipe a una associazione (reclusione di 5 anni); l'addestratore e l'addestrato sono puniti come il partecipe a una associazione (reclusione da 5 a 10 anni).

Per quanto riguarda poi le misure di prevenzione[12], con la riforma del 2015 la fattispecie soggettiva di pericolosità prevista dall'art. 4, comma 1, lett. d) del Codice Antimafia, risulta riferibile non soltanto a coloro che, operanti in gruppi o isolatamente pongano in essere atti

[12] In argomento v. per tutti A. BALSAMO, *Le modifiche in materia di misure di prevenzione e di espulsione degli stranieri*, in AA.VV., *Il nuovo "pacchetto" antiterrorismo*, cit., 21 ss.

preparatori, obiettivamente rilevanti, diretti alla commissione dei reati con finalità di terrorismo anche internazionale (testo vigente prima della riforma), ma anche a coloro che pongano in essere atti preparatori, obiettivamente rilevanti, diretti a prendere parte ad un conflitto in territorio estero a sostegno di un'organizzazione che persegue finalità terroristiche di cui all'art. 270-*sexies* del codice penale (testo aggiunto con la riforma).

Ebbene, non si può fare a meno di osservare come anche questa riforma si caratterizzi per una certa confusione tra dimensione bellica e dimensione criminale, in quanto, da un lato, si fa riferimento al fatto che si realizzino atti per prendere parte a un conflitto, mentre dall'altro, si fa riferimento al sostegno ad una organizzazione criminale che persegue finalità terroristiche.

Ma al di là di questo profilo, il nodo di fondo che si deve affrontare è il ruolo e il significato che assumono le misure di prevenzione nel nostro sistema. Ebbene, anzitutto si deve avere il coraggio di riconoscere che il sistema delle misure di prevenzione è un sistema che appartiene alla logica dell'emergenza, soprattutto se poi esso si ispira non tanto al modello basato sulla pericolosità soggettiva del destinatario della misura, ma piuttosto al modello basato su un sospetto di reato tipizzato. In secondo luogo, si deve osservare che purtroppo tale sistema, essendo strutturale, sembra essere divenuto un vero e proprio strumento di uno stato di eccezione all'interno dello Stato di diritto: mafia, e a quanto pare ormai anche il terrorismo, sembrano creare le condizioni di un'emergenza nella sostanza interminabile. Se quanto affermato è vero, si deve allora avere ancor più coraggio e iniziare ad affermare che rispetto al sistema delle misure di prevenzione, se possono essere derogati alcuni principi, tuttavia non possono essere derogati i principi per l'appunto inderogabili, compreso il principio di irretroattività, che tuttavia, com'è noto, la giurisprudenza non ritiene operante. Infine, si deve evidenziare come in una prospettiva di riforma, ammesso e non sempre concesso che organizzazioni mafiose e organizzazioni terroristiche possano essere assimilate, è comunque rispetto alla criminalità organizzata che si può giustificare una anticipazione della tutela in termini indiziari, mentre dovrebbero essere eliminate tutte le ipotesi che si riferiscono a reati "monosoggettivi". Ma è noto come il legislatore si stia muovendo

proprio nella esatta direzione opposta, volendo addirittura applicare il sistema delle misure di prevenzione ai sospettati di delitti contro la pubblica amministrazione.

## *7. Considerazioni conclusive*

Rispetto al terrorismo si devono distinguere obiettivi e mezzi simbolici e obiettivi e mezzi reali. Simbolico è l'obiettivo di sovvertire un sistema dall'esterno, così come simbolico è alla fin fine lo strumento della violenza. Potrà sembrare un paradosso, ma non lo è: la violenza terroristica, espressa da organizzazioni criminali, non è mai in grado di per sé di raggiungere direttamente l'obiettivo di sovvertire un sistema.

Reale è invece l'obiettivo di dissolvere la democrazia dall'interno e il mezzo reale per raggiungere questo obiettivo è la democrazia stessa. In ultima analisi, il terrorismo non fa altro che avvalersi della democrazia per dissolverla dall'interno. Il terrorismo è un fenomeno che attraverso la violenza tende a far scoppiare le contraddizioni interne alla democrazia, a minare la stessa fiducia che i consociati hanno in essa e nei valori per i quali il terrorismo si contrasta. In sostanza, il terrorismo non tende alla dissoluzione del sistema, ma alla sua autodissoluzione.

Ecco allora emergere il vero volto alla lotta al terrorismo. Certo, lotta delle democrazie contro le organizzazioni criminali, ma anche, e direi soprattutto, lotta della democrazia contro se stessa, contro le sue pulsioni ad autodistruggersi per contrastare il terrorismo. E non esiste lotta più dura e difficile quando il nemico, alla fin fine, è rappresentato da noi stessi.

# "EMERGENZA TERRORISMO": STRATEGIE DI PREVENZIONE E CONTRASTO ANCHE IN PROSPETTIVA EUROPEA

*Ilaria Marchi*

SOMMARIO*: 1. Considerazioni introduttive. 2. Natura del fenomeno, difficoltà definitorie e rapporti con la sicurezza. 2.1. Il paradigma bellico della sicurezza e la normalizzazione dell'emergenza nell'esperienza dello Stato di Israele. 2.2. L'approccio europeo e il paradigma della sicurezza basato sul c.d.* Law Enforcement*. 3. Luci ed ombre del progetto di direttiva per il contrasto al terrorismo. 4. Conclusioni: verso un nuovo paradigma extra-sistemico della sicurezza?*

## *1. Considerazioni introduttive*

Il fenomeno terroristico ha acquisito ormai rilevanza su scala mondiale, rendendo non più differibile lo sviluppo di una strategia di sicurezza in grado di adeguarsi alle diverse dimensioni in cui esso può articolarsi, nonché un ripensamento degli strumenti giuridici di prevenzione e di contrasto implementati a livello nazionale e sovranazionale.

Negli ultimi anni, infatti, si è assistito ad una *escalation* di attacchi terroristici e, allo stesso tempo, ad una modifica del *modus operandi* impiegato: dagli attentati effettuati con l'utilizzo di ordigni esplosivi, si è passati all'utilizzo di terroristi suicidi. Sono state messe in campo anche strategie tipiche dei commando militari, apprese in campi di addestramento creati *ad hoc* in alcuni paesi del Medio-oriente (tra cui Iraq, Arabia Saudita e Siria) e, da ultimo, si è dato l'avvio all'utilizzo di attacchi informatici potenzialmente distruttivi ed effettuati a danno di infrastrutture sensibili, come accaduto nella "vicenda Centcom", in relazione alla quale si è parlato di Cyberterrorismo e di *Cyberjihad*[1].

[1] Il riferimento va all'attacco hacker perpetrato il 12 gennaio 2015 dai militanti dell'ISIS a danno della banca-dati e dell'account twitter @Centcom del Comando statuni-

La necessità di introdurre modifiche al sistema normativo antiterrorismo è apparsa urgente dopo le drammatiche vicende francesi, belghe e turche[2]. Il terrorismo, in particolare di matrice islamica, ha iniziato a colpire in modo diretto e sistematico l'Europa, soprattutto attraverso azioni di giovani reclutati e radicalizzati *on-line*, attraverso *blog* e siti dedicati alla propaganda *jihadista*[3].

Le reazioni dei governi francese e turco sono state fra le più decise: entrambi, infatti, hanno immediatamente azionato la clausola dell'art. 15 della Convenzione europea dei diritti dell'uomo (CEDU), notificando al Consiglio d'Europa la propria volontà di istituire uno "stato di eccezione". Ne sono stata immediata conseguenza i *raid* aerei sui territori controllati dall'ISIS e la richiesta da parte della Francia di un intervento congiunto degli Stati membri, nel quadro dell'art. 42 comma 7 del Trattato sull'Unione europea (TUE)[4].

---

tense che controlla le operazioni contro lo Stato islamico in Siria ed Iraq. Per una disamina del nuovo fenomeno v. R. FLOR, *Il contrasto al terrorismo nell'era delle nuove tecnologie e i meccanismi di cooperazione fra settore pubblico e settore privato*, in M. MANTOVANI, F. CURI et al., *Scritti in onore di Luigi Stortoni*, Bologna, 2016, 513-546; più ampiamente v. U. SIEBER, P. BRUNST, *Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions*, Strasbourg, 2007.

[2] Dopo l'assalto alla redazione del giornale satirico Charlie Hebdo, nel novembre del 2015 la Francia è stata nuovamente colpita da cruente sparatorie nelle zone del I, X e XI *arrondissement* di Parigi ed in particolare al teatro Bataclan; in Belgio si è registrato l'attacco esplosivo all'aeroporto di Bruxelles e nella stazione della metropolitana di Maalbeek; in Turchia, le esplosioni nell'aeroporto di Istanbul e nella zona di Taxim; con il medesimo *modus operandi* del tir gettato in corsa sulla folla la strage di 84 persone sulla *promenade* di Nizza ed il recente attacco a Berlino.

[3] Cfr. i dati raccolti nello studio effettuato da J. KLAUSEN, *Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq*, in *Studies in Conflicts & Terrorism*, 2014, vol. 38, 1-22. Dal monitoraggio dell'account *Twitter* di 59 combattenti dislocati in Siria, nel trimestre gennaio-marzo 2014 risultano essere stati postati 159.112 *Tweet*. In media ogni account ha caricato 85 immagini e 91 filmati aventi contenuto religioso, di aggiornamento sullo stato del conflitto e sulle tecniche di guerra per lo sterminio degli infedeli. 4 *Tweet* su 5 facevano riferimento al dogma *jihadista*.

[4] L'art. 42 comma 7 recita: «tutti gli Stati membri sono tenuti a dare aiuto e assistenza a uno qualsiasi degli altri Stati che abbia subito un'aggressione armata, in conformità con l'art. 51 della carta delle Nazioni Unite». Un chiaro ritorno alla configura-

Il tema della *international security* e dei suoi rapporti con i diritti fondamentali entra dunque di diritto tra le priorità delle agende strategiche nazionali e sovranazionali. Nonostante l'efferatezza della minaccia e il costante richiamo alla necessità di innalzare il livello di sicurezza da garantire ai cittadini, il tentativo di riconoscere a quest'ultima un ruolo in chiave sia repressiva, sia di prevenzione dei fenomeni di criminalità particolarmente grave, è comunque guardato con sospetto. Infatti, il concetto di *security* è tradizionalmente ritenuto talmente fluido da poter essere manipolato dai governi per ottenere poteri straordinari, se non sproporzionati, rispetto al reale grado della minaccia, da esercitare al di fuori dei tradizionali controlli effettuati dalle Corti[5].

Malgrado queste resistenze, a livello europeo pare ormai essersi consolidato un vero e proprio diritto alla sicurezza[6], da intendersi come diritto dello Stato quale struttura essenziale per la collettività e come diritto alla vita ed alla integrità fisica dei cittadini, destinato ad acquisire un ruolo rilevante sia a livello di politica criminale, sia in relazione alla valutazione di costituzionalità (*rectius*: necessità e proporzionalità) di misure limitative delle libertà fondamentali. Di fatto, le scelte di criminalizzazione che si stanno sviluppando nell'alveo dell'art. 83 del Trattato sul Funzionamento dell'Unione europea (TFUE), non possono che venire interpretate come stimolo per il superamento delle tradizio-

zione del terrorismo come atto di guerra ed alla esigenza di operare nel quadro della politica estera e di sicurezza comune, sul presupposto della azionabilità della legittima difesa dello Stato. Si è scelto consapevolmente di non menzionare la clausola di solidarietà dell'art. 222 TFUE, che in caso di attacco terroristico contro uno Stato membro prevede un'azione congiunta a livello europeo, eventualmente con l'impiego di mezzi militari, non necessariamente quale premessa ad una dichiarazione di guerra ma anche al solo fine di ripristinare l'ordine e rafforzare i controlli.

[5] Più ampiamente: v. B. ACKERMAN, *Prima del prossimo attacco: preservare le libertà civili in un'era di terrorismo globale*, Milano, 2008, 66 ss. (ID., *Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism*, London, 2006, tr. it. di A. QUARENGHI).

[6] Sul punto si permetta il richiamo a I. MARCHI, *Esigenze di sicurezza e diritti umani nel contrasto al terrorismo. Una prospettiva* de iure condendo, in *Dir. pen. XXI sec.*, 2015, vol. 2, 259-278.

nali resistenze delle "anime belle"[7], da sempre contrarie ad ogni tentativo di rendere effettivo il diritto alla sicurezza.

Pare essere giunto il momento di riflettere in modo responsabile su nuove politiche multilivello di prevenzione e contrasto al terrorismo, inteso quale fenomeno che opera ormai su scala mondiale e che possiede tratti di micidialità idonei a porre in pericolo non solo vite umane ma la stessa sopravvivenza degli Stati.

In questo breve contributo, partendo dalla definizione di due paradigmi, uno di natura bellica ed il secondo detto di *Law Enforcement*, ci si propone di fornire una possibile ricostruzione del ruolo della sicurezza nel settore della "lotta" al terrorismo, anche alla luce della proposta di direttiva adottata dall'Unione nel dicembre 2015, sulla base dell'art. 83 TFUE[8]. Richiamando l'attenzione sulle lacune del progetto normativo, da ultimo, si riflette sul possibile sviluppo di un terzo paradigma, di natura extra-sistemica, che rischierebbe di vanificare gli sforzi effettuati a tutela dello Stato di diritto.

## *2. Natura del fenomeno, difficoltà definitorie e rapporti con la sicurezza*

L'assetto attuale della lotta al terrorismo a livello internazionale rischia, di fatto, di creare gravi commistioni tra diritto e guerra, nonché pericolose sovrapposizioni tra categorie, dovute soprattutto alla difficoltà che la Comunità internazionale è stata chiamata a fronteggiare nel fornire una definizione giuridica condivisa del fenomeno.

Guardando alle decisioni adottate dagli Stati subito dopo un attacco terroristico, è possibile identificare due gradi di reazione: la prima fase contempla il richiamo a concetti di natura bellica, mentre la seconda, influenzata in genere dalla fondamentale opera delle Corti, tende verso

[7] Così F. BATTISTELLI, *La sicurezza e la sua ombra. Terrorismo, panico, costruzione della minaccia*, Roma, 2016, 39-40, che per le sue considerazioni richiama il tipo umano definito "anima bella" da Hegel nella sua opera *Fenomenologia dello spirito*.

[8] Vedi COM(2015) 625 final, *Proposal for a Directive on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism*, reperibile on-line: *https://ec.europa.eu*.

il reinserimento della minaccia tra quelle che tipicamente il diritto penale è chiamato a reprimere.

Tale quadro, dunque, conferma l'intuizione di alcuni autori che, lungi dall'effettuare una netta scelta di campo, hanno preferito definire il terrorismo come un «super-reato»[9], in modo da attrarre le caratteristiche sia del diritto, sia della guerra.

Un esempio delle difficoltà trovate nel formulare una definizione giuridica condivisa di "terrorismo" è offerto dai lavori del Comitato istituito dall'Assemblea Generale dell'ONU, per la stesura di una Convenzione globale sul terrorismo, che dopo vent'anni ancora non ha visto la luce. Tra i punti maggiormente critici, infatti, si annovera l'ampio dibattito circa l'opportunità di riconoscere una esimente a favore dei c.d. *freedom-fighters*[10], ipotesi largamente osteggiata da parte degli Stati occidentali per il timore di introdurre una "clausola di impunità" a favore di soggetti che, pur esercitando un diritto legittimo, operano al di fuori delle regole previste dalle Convenzioni di Ginevra[11], strumento forse non più adatto a regolare scenari di "guerra asimmetrica" o "ibrida"[12].

---

[9] Il riferimento va a G.P. FLETCHER, *I fondamenti filosofico-giuridici della repressione del terrorismo*, in M. DONINI, M. PAPA (a cura di), *Diritto penale del nemico: un dibattito internazionale*, Milano, 2007, 371. Vedi anche ID., *The Indefinable Concept of Terrorism*, in *J. Int'l Crim. Just.*, 2006, 894-911.

[10] Vedi l'art. 18, comma 2, del progetto di Convenzione globale. In argomento cfr. R. BARBERINI, *Terrorismo e movimenti di liberazione nazionale: la Convenzione globale contro il terrorismo*, in A. DE GUTTRY (a cura di), *Oltre la reazione. Complessità e limiti nella guerra al terrorismo internazionale dopo l'11 settembre*, Pisa, 2003, 107 ss.

[11] Per un approfondimento: v. G. NESI, *International Terrorism, the Law of War and the Negotiation of a UN Comprehensive Convention*, in F. POCAR, M. PEDRAZZI, M. FRULLI (a cura di), *War Crimes and the Conduct of Hostilities. Challenges to Adjudication and Investigation*, Cheltenham (UK), 2013, 243-256.

[12] Basti pensare alla categoria degli *unlawful enemy combatants* (nell'accezione statunitense), quale categoria ibrida di soggetti, non inquadrabili né tra i civili, né tra i combattenti legittimi, creata *ad hoc* per sottrarli all'applicazione delle Convenzioni di Ginevra. Sul punto: T.D. GILL, E. VAN SLIEDREGT, *Guantanamo Bay: a Reflection on the Legal Status and Rights of "Unlawful Enemy Combatants"*, in A.M. HOLE, J. VERVAELE, *Security and Civil Liberties: The Case of Terrorism*, Oxford, 2005, 1 ss. Per una disamina critica delle problematiche connesse a tale distinzione v. R. BARTOLI, *Le nuo-*

Tale impostazione sembra oggi non più negoziabile alla luce delle previsioni della Risoluzione ONU n. 2178/2015[13], che prevede espressamente un obbligo di incriminazione dei c.d. *foreign terrorist fighters*[14], per arginare il fenomeno definito *blowback*, ovvero di addestramento in Stati stranieri di combattenti da impiegare nella commissione di attacchi terroristici in Europa.

Ad essa ha poi fatto seguito l'adozione da parte del Consiglio d'Europa del Protocollo addizionale alla Convenzione europea per la prevenzione del terrorismo[15], che riprende gli obblighi di criminalizzazione della risoluzione appena citata, poi trasposti nel progetto di direttiva per il contrasto al terrorismo, oggi in discussione in seno all'Unione[16].

### *2.1. Il paradigma bellico della sicurezza e la normalizzazione dell'emergenza nell'esperienza dello Stato di Israele*

Guardando al panorama internazionale, la commistione tra diritto e guerra non è solo un'ipotesi astratta ma ha già avuto ampi riscontri, primo tra tutti quello che si ricava dall'esperienza dello Stato di Israele, ove tale tendenza è divenuta ormai sistemica. Il complesso e stratificato sistema normativo antiterrorismo israeliano, infatti, è caratterizzato da una dimensione dinamica di lotta, dominata dallo *jus ad bellum*, funzionale al richiamo alla legittima difesa preventiva di cui all'art. 51 del-

*ve emergenze terroristiche: il difficile rapporto tra esigenze di tutela e diritti umani*, in questo volume.

[13] Cfr. art. 6 lett. a) S/RES/2178(2014), adottata dal Consiglio di Sicurezza il 24 settembre 2014, reperibile on-line: *www.un.org*. Per un commento critico alla risoluzione v. M. SOSSAI, Foreign Terrorist Fighters*: una nozione ai confini del diritto internazionale*, in *federalismi.it*, 2015.

[14] Sul punto: A. ALÌ, *La risposta della Comunità internazionale al fenomeno dei Foreign Terrorist Fighters*, in *La Comunità int.*, 2015, 181-201.

[15] Il Protocollo addizionale è stato aspramente criticato da Amnesty International e dalla International Commission of Jurists, nel documento del 6 marzo 2015, dal titolo: *Preliminary public observations on the terms of reference to draft an Additional Protocol supplementing the Council of Europe Convention on the Prevention of Terrorism*. Testo reperibile on-line: *www.amnesty.org*.

[16] Vedi *infra*, par. 3.

la Carta ONU, e da una statica, votata all'utilizzo di misure amministrative, oltre che al richiamo al diritto penale[17].

Tale quadro viene reso ancora più complesso dalla coesistenza di leggi che fanno dipendere la propria vigenza dal rinnovo dello stato di emergenza, in assenza del quale esse diventerebbero inapplicabili. Ne sono un esempio la *Criminal Procedure (Detainee Suspected of Security Offence) (Temporary Provision) Law 5766/2006*, la *Emergency Powers (Detention) Law 1979* e la *Prevention of Terrorism Ordinance 5708-1948*[18] che, in combinato disposto con la legge contro il finanziamento alle organizzazioni criminali, fornisce una definizione di organizzazione terroristica, delinea le figure del partecipe e del favoreggiatore e contiene previsioni in ordine alle condotte di supporto punibili, all'onere della prova, alle varie ipotesi di confisca.

Porre fine allo stato di emergenza, dunque, avrebbe come effetto immediato la creazione di un *legal vacuum* all'interno dell'ordinamento, che farebbe perdere efficacia ad una fetta consistente della legislazione antiterrorismo. Proprio siffatta consapevolezza ha contribuito a rendere la perpetuazione dell'emergenza una pericolosa questione di natura politica, considerato che la dichiarazione dello stato di emergenza, in tale ordinamento, non è vincolata a specifici presupposti ed ha effetti generali sul sistema[19].

Al fine di superare questo *impasse*, anche grazie alle raccomandazioni della Corte Suprema[20], il 9 giugno 2013 il Comitato ministeriale

---

[17] Più ampiamente: v. C. KLEIN, *On the Three Floors of a Legislative Building: Israel's Legal Arsenal in its Struggle against Terrorism*, in *27 Cardozo L. Rev.*, 2005-2006, 2223 ss.

[18] Per una breve disamina si rinvia a E.M. SALZBERGER, *Counterterrorism Law in Israel*, 2016, on-line: *http://minervaextremelaw.haifa.ac.il/*. Si permetta altresì il rinvio a I. MARCHI, *Stato di eccezione e sovvertimento delle regole: alcune riflessioni sul sistema israeliano antiterrorismo*, in S. BONINI, L. BUSATTA, I. MARCHI (a cura di), *L'eccezione nel diritto*, Napoli, 2015, 275-280.

[19] Per un approfondimento v. S. NAVOT, *The Constitutional Law of Israel*, Alphen aan den Rijn (NL), 2007, 293 ss.

[20] Preme ricordare che nel 1999 l'*Association for Civil Rights in Israel (ACRI)* decise di ricorrere alla *High Court of Justice* affinché venisse valutata la legittimità dei continui rinnovi dello stato di emergenza ed eventualmente ne venisse disposta la revoca. La Corte con la sentenza 3091/99, *The Association for Civil Rights in Israel v. The*

per la legislazione ha finalmente dato avvio ad un progetto organico di riforma, il *Counter Terrorism Bill 5775-2015*[21], approvato in via definitiva il 15 giugno 2016 ed entrato in vigore l'1 novembre 2016. Ad esso ha fatto seguito la c.d. *Facebook Law*, approvata in prima lettura dalla Knesset il 3 gennaio 2017 e destinata ad obbligare *provider* e *social media* ad adeguarsi agli ordini di rimozione emessi dalle Corti israeliane, in caso di pubblicazione di contenuti ritenuti rilevanti a fini di propaganda, istigazione a delinquere, organizzazione di attacchi e arruolamento.

In sede di lavori preparatori, la riforma della legislazione di settore era stata salutata con favore, quale occasione per giungere ad un ripensamento sistemico, legato soprattutto ad un nuovo vaglio di proporzionalità delle misure antiterrorismo rispetto alla tutela dei diritti umani. Ad oggi, tuttavia, le discussioni che hanno accompagnato il progetto della nuova legge paiono aver sortito il solo effetto di sedimentare l'emergenza nell'ordinamento, trasponendo senza modifiche in legge nazionale non solo alcuni *temporary order* dell'esecutivo, ma anche numerose misure draconiane e di natura prettamente amministrativa,

*Knesset and the Government of Israel*, dell'8 maggio 2012 decise di rigettare il ricorso raccomandando al Parlamento di porre fine a tale situazione, trasponendo le leggi dipendenti dallo stato di emergenza in leggi ordinarie da esso indipendenti. Per un commento: v. J. REYNOLDS, *"Intent to regularise": The Israeli Supreme Court and the Normalisation of Emergency*, in *Adalah's Newsletter*, vol. 104, 2013.

[21] Per un breve riassunto in lingua inglese v.: *www.justice.gov.il*. Per un commento si rimanda a U.B. YAAKOV, D. HAREL, *Policy Paper: Israel's Counter Terrorism Bill*, IDC Herzliya, 2016, dove vengono criticate alcune scelte di politica criminale, tra cui (senza pretesa di esaustività): 1) la facoltà concessa al Ministro della difesa di individuare *Terrorist Infrastructure Zones*, utili a creare presunzioni di colpevolezza in relazione a coloro che vi operano; 2) l'omessa distinzione, anche sul piano sanzionatorio, tra coloro che appartengono ad organizzazioni terroristiche primarie e membri di organizzazioni di mero supporto logistico o finanziario; 3) la non oggettività dei criteri individuati per la prova della partecipazione in un gruppo terroristico; 4) la procedura di *listing*; 5) la mancanza di criteri chiari per l'ascrizione del ruolo rivestito da ciascuno nel gruppo criminale; 6) l'obbligo di punire anche la mera connivenza o la semplice adesione alle motivazioni da cui muove anche uno solo degli attacchi.

previste dalle *Defence (Emergency) Regulations* del 1945[22], ereditate dal mandato britannico sulla Palestina.

In particolare, il *Counter Terrorism Bill 5775-2015* riprende formule vaghe e generiche per la definizione di cosa si intenda per terrorismo e circa i requisiti strutturali necessari affinché un gruppo terroristico possa venire definito tale, introducendo nuove fattispecie di reato legate all'istigazione ed alla apologia del terrorismo che non possono non risentire di tale carenza di precisione. Esso ha poi ampliato i poteri di polizia e dei servizi segreti, ha esteso i casi di legittimo utilizzo di prove segrete e abbassato lo standard probatorio necessario per la condanna in procedimenti legati alle c.d. *security offences* (tra cui oggi si annovera anche il lancio di pietre, punito grazie ad un *temporary order*, intervenuto a modifica del codice penale il 2 novembre 2015 ed efficace sino al 2018, salvo rinnovo)[23].

La novella appena richiamata, dunque, ricalca i tratti di quello che è stato chiamato *Business as usual Model*[24], che prevede l'implementazione di misure emergenziali e straordinarie all'interno dell'ordinamento, con l'effetto di normalizzare l'eccezione, rendendola in tal modo regola.

La matrice securitaria che ha caratterizzato tali scelte di politica criminale rischia di riversarsi sulla futura ermeneutica delle Corti di merito, e dei Tribunali militari. Solo la Corte Suprema israeliana potrebbe ergersi a baluardo di tutela dei diritti umani, posto che si è tradizionalmente adoperata, soprattutto durante la presidenza di Aaron Barak, per sottoporre le misure adottate dal governo nel quadro della "lotta al terrorismo" ad uno stringente *test* di proporzionalità, vincolando ad

[22] Per un commento al primo *draft* vedi la sintesi critica offerta dall'Israel Democracy Institute (IDI), *New Comprehensive Counter-terrorism Memorandum Bill*, on-line: *www. en. idi. org.il*; v. anche il *position paper* preparato per la *Association for Civil Rights in Israel* dall'*Attorney* L. Margalit, reperibile on-line: *www.acri.org.il*.

[23] Cfr. il *report* di *Adalah* dal titolo: *Israel: New Discriminatory and Anti-Democratic Legislation*, 1 marzo 2016, on-line: *www.adalah.org*.

[24] Il riferimento va a O. GROSS, *Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?*, in *112 Yale L. J.*, 2003, 1043 ss.

una *zone of reasonableness* addirittura la discrezionalità dei *Military Commanders*, operanti all'interno dei territori occupati[25].

Il vaglio di legittimità così introdotto può di fatto venire superato solo se la misura oggetto di giudizio risulta essere: 1) idonea a raggiungere lo scopo prefissato; 2) la meno invasiva rispetto a quelle astrattamente applicabili; 3) quella che garantisce un corretto rapporto di proporzionalità[26].

Bisogna comunque dare atto che tale pregevole, ma purtroppo solo teorica, costruzione ha scontato l'impatto con la realtà, assumendo i caratteri tipici del paradigma bellico della sicurezza. I giudici supremi, infatti, fondano oggi le proprie decisioni su un concetto di *national security* pericolosamente fluido, delineato secondo le clausole eccezionali del diritto internazionale umanitario, che portano a riconoscere la sicurezza nazionale come bene prevalente nel meccanismo di *checks and balances*[27]. Lo stesso criterio ermeneutico di proporzionalità, utilizzato per verificare la legittimità della misura rispetto alla protezione del diritto fondamentale da essa interessato, pare possedere una matrice bellica, considerato che la valutazione viene parametrata al grado di beneficio militare raggiunto, a nulla rilevando il numero di "vittime collaterali" colpite[28]. Al contrario, se per la medesima decisione venisse utilizza-

[25] Anche per la bibliografia richiamata v. E. GROSS, *Fighting Terrorism with one Hand Tied Behind the Back: Delineating the Normative Framework for Conducting the Struggle Against Terrorism within a Democratic Paradigm*, in *29 Wis. Int'l L.J.*, 2011, 23 ss.

[26] Cfr. HCJ, 2056/04, *Beit Sourik Village Council v. the Government of Israel*. Tale test, sconta però una "stortura" preliminare ovvero l'esistenza di una presunzione, seppur relativa, di buona fede dei *Military Commanders* nella scelta della strategia antiterrorismo da utilizzare, sulla scorta del fatto che tali soggetti possono vantare uno specifico *know-how* in materia di sicurezza. Cfr. HCJ 258/79, decisione reperibile solo in ebraico.

[27] Per un commento: v. M. ROSENFELD, *Judicial Balancing in Time of Stress*, in T. GROPPI (a cura di), *Democrazia e Terrorismo*, Napoli, 2006, 166 ss.; più di recente A. REICHMAN, *Judicial Independence in Times of War: Prolonged Armed Conflict and Judicial Review on Military Action in Israel*, in *Utah L. Rev.*, 2011, 77 ss.

[28] Sul punto: v. A. GIOIA, *Lotta al terrorismo, diritto di guerra e diritti dell'uomo*, in P. GARGIULO, M.C. VITUCCI (a cura di), *La tutela dei diritti umani nella lotta e nella guerra al terrorismo*, Napoli, 2009, 191 ss. Il fatto che in tempo di guerra spetti al diritto umanitario stabilire quando la privazione della vita sia arbitraria è stato confermato

to, quale *tertium comparationis*, quanto previsto dalle Convenzioni internazionali a tutela dei diritti umani – tra cui ad esempio CEDU e Patti civili e politici di New York – in relazione soprattutto ai livelli minimi di tutela da garantire alle libertà fondamentali, il giudizio di ragionevolezza finale sarebbe certamente diverso. Il *test* di proporzionalità da effettuare, infatti, implicherebbe l'utilizzo, quale secondo polo del giudizio di bilanciamento tra interessi contrapposti, il grado massimo tollerabile di invasività della misura adottata rispetto al diritto che ne viene colpito[29].

### *2.2. L'approccio europeo e il paradigma della sicurezza basato sul c.d.* Law Enforcement

Il secondo paradigma della sicurezza, opposto a quello bellico caratterizzante il sistema israeliano, può essere definito di *Law Enforcement*, poiché prevede che il terrorismo venga trattato come fenomeno esclusivamente criminale e che la strategia di contrasto venga costruita sulla interazione costante tra diversi rami del diritto: sulla cooperazione giudiziaria e di *intelligence* nella fase di prevenzione e di controllo delle attività dei presunti terroristi, e sul diritto penale nella fase repressiva[30].

Concentrando l'attenzione sul *trend* che in questi anni si è sviluppato nel contesto europeo, confermato anche dopo i più recenti attacchi, si possono enucleare alcune costanti tra le reazioni immediate offerte dagli Stati nella lotta al terrorismo.

---

anche dalla Corte internazionale di giustizia nella *Advisory Opinion* pronunciata l'8 luglio 1996: ICJ, *Legality of the Threat or Use of Nuclear Weapons*, par. 25, on-line: *http://www.icj-cij.org*.

[29] Cfr. *Benzer and others v. Turkey* (Appl. no. 23502/06), on-line: *http: // hudoc. echr.coe.int*. Cfr. anche le valutazioni in termini di proporzionalità offerte dall'Avvocato generale Villalòn, nelle conclusioni depositate il 12 dicembre 2013 alla Corte di giustizia, nella causa *Digital Rights Ireland Ltd* C-293/12.

[30] Sul punto: U. SIEBER, *Blurring the Categories of Criminal Law and the Law of War: Efforts and Effects in the Pursuit of Internal and External Security*, in S. MANACORDA, A. NIETO MARTÍN (a cura di), *Criminal Law Between War and Peace – Justice and Cooperation in Criminal Matters in International Military Interventions*, Cuenca (ES), 2009, in particolare 64 ss.

Da un lato, sul piano processuale si è assistito ad un aumento dei poteri investigativi e di polizia che, grazie soprattutto all'utilizzo delle nuove tecnologie, sono stati resi sempre più invasivi rispetto ai diritti non solo degli indagati ma anche a quelli dei cittadini[31], nonché ad un rafforzamento dei poteri di *intelligence*, attraverso l'estensione delle c.d. scriminanti funzionali legate alle attività dei servizi segreti[32] e l'autorizzazione per procedere con la c.d. *strategic surveillance*[33]. Dall'altro lato, sul piano del diritto penale sostanziale, grazie anche alla spinta sovranazionale[34], si è assistito alla adozione di fattispecie incriminatrici connotate da una forte anticipazione di tutela, nonché da formulazioni spesso generiche, che fanno ampio ricorso al dolo specifico. Infatti, già a partire dal 2015, a seguito della risoluzione ONU n. 2178/2015 e del Protocollo addizionale del Consiglio d'Europa, numerosi Stati europei hanno introdotto nel proprio sistema incriminazioni finalizzate alla repressione di condotte prodromiche a quelle di attentato, quali l'istigazione a commettere atti di terrorismo, il reclutamento, l'addestra-

[31] Cfr. M.L. DI BITONTO, *Terrorismo internazionale, procedura penale e diritti fondamentali in Italia*, in *Cass. pen.*, 2012, 1186. Nel panorama internazionale v. E. VIANO, *Balancing Liberties and Security Fighting Cybercrime: Challenges for the Networked Society*, in S. MANACORDA, R. FLOR, J. OH JANG (a cura di), AA.VV., *Cybercriminality: Finding a Balance between Freedom and Security*, Milano, 2012, 33 ss.

[32] Il rafforzamento dei poteri di *intelligence* rappresenta un tratto comune nelle recenti leggi anti-terrorismo di Francia (Loi n. 2015-912, approvata il 24 giugno 2015), Gran Bretagna (in particolare con l'emendamento al *Computer Misuse Act*, introdotto dal *Serious Crime Act 2015*, approvato il 3 marzo 2015 che ha previsto una clausola di immunità a favore non solo dei membri dei servizi segreti ma anche alle autorità investigative in caso di indagini altamente tecnologiche) ed Italia (emendamenti alla legge 124/2007 introdotti dall'art. 8 della legge n. 43/2015).

[33] Con tale definizione ci si riferisce alle *bulk interceptions*, che prevedono l'utilizzo di tecniche idonee a raccogliere una mole indiscriminata di dati, anche in assenza di indizi di reato, che vengono poi filtrati attraverso appositi algoritmi, al fine di selezionare notizie ritenute utili. Per una disamina della compatibilità di tale strumento, previsto dal *Regulatory Investigatory Powers Act* inglese con il diritto alla *privacy* v. Corte europea dei diritti dell'uomo, *10 Human Rights Organisations v. the United Kingdom*, Application n. 24960/15, 20 maggio 2015, on-line: *www.hudoc.echr.coe.int*.

[34] Di recente: *Council of Europe, Committee on Foreign Terrorists Fighters and Related Issues, Draft Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism*, 12 marzo 2015, on-line: *https://www.coe.int*.

mento, accompagnati da previsioni *ad hoc* per il contrasto al sempre crescente numero di *foreign fighters*[35].

Guardando alle modifiche introdotte dal legislatore italiano, dapprima con il decreto-legge n. 7/2015, convertito nella legge 43/2015 e, successivamente, con la legge n. 153/2016 di adeguamento ad alcuni strumenti internazionali in attesa di ratifica[36], si nota come il nostro sistema giuridico abbia attraversato tutte le fasi caratterizzanti il *trend* europeo sopra descritto.

Al complesso micro-sistema di diritto sostanziale per il contrasto al terrorismo sono state aggiunte nuove fattispecie incriminatrici[37]: l'art. 270-*quater.1* c.p., che punisce la "organizzazione di trasferimenti con finalità di terrorismo", l'art. 270-*quinquies.1* c.p. che punisce il finanziamento di condotte con le medesime finalità, l'art. 270-*quinquies.2* c.p. ovvero la sottrazione di beni o denaro sottoposti a sequestro e infine l'art. 280-*ter* c.p. rubricato "Atti di terrorismo nucleare". Altre fattispecie hanno subito modifiche finalizzate ad ampliarne la portata applicativa: questo è il caso dell'art. 270-*quater* c.p., che prevede oggi la punibilità anche del soggetto arruolato, nonché dell'art. 270-*quinquies* che colpisce anche il soggetto che si auto-addestra, raccogliendo autonomamente informazioni per compiere atti con univoca finalità terroristica[38].

---

[35] Cfr. il *report* stilato da Europol, *European Union Terrorism Situation and Trend Report 2016*, reperibile on-line: *www.europol.europa.eu*.

[36] Il riferimento va alla risoluzione ONU n. 2178/2014, alla Convenzione di Varsavia per la prevenzione del terrorismo (2005), alla Convenzione di New York per soppressione di atti di terrorismo nucleare (2005), alla Convenzione di Varsavia sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo (2005), al Protocollo di emendamento alla Convenzione europea per la repressione del terrorismo (2003) nonché al Protocollo addizionale alla Convenzione del Consiglio d'Europa per la prevenzione del terrorismo (2015).

[37] Per un commento v. G. LEO, *Nuove norme in materia di terrorismo*, in *www.penalecontemporaneo.it*, 2015; S. COLAIOCCO, *Prime osservazioni sulle nuove fattispecie antiterrorismo introdotte dal decreto-legge n. 7 del 2015*, in *Arch. pen.*, 2015, 1 ss.; F. FASANI, *Il decreto antiterrorismo: una prima lettura*, in *Dir. pen. e proc.*, 2015, 918 ss.; per un maggiore approfondimento ID., *Terrorismo islamico e diritto penale*, Padova, 2016.

[38] Per una panoramica v. A. VALSECCHI, *Le modifiche alle norme incriminatrici in materia di terrorismo*, in E. KOSTORIS, F. VIGANÒ, *Il nuovo 'pacchetto' antiterrorismo*, Tori-

Vero è che questi interventi hanno sollevato ampie critiche in relazione al mancato rispetto dei principi di determinatezza e di offensività, minati dalla stessa formulazione dell'art. 270-*sexies* c.p. che, non a caso, è stata definita una previsione «parzialmente in bianco e (…) insoddisfacente sotto il profilo della determinatezza»[39] e dunque insidiosa per l'interprete se si ritiene che essa concentri in sé l'intero disvalore penale di condotte altrimenti neutre[40]. Parte della dottrina ha richiamato anche il concetto di diritto penale simbolico e «del mero sospetto di autore»[41], viste le difficoltà probatorie connesse ad esempio alle condotte di arruolamento, addestramento (che difficilmente acquista autonomia rispetto alla partecipazione già punita dall'art. 270-*bis* c.p.) ed ora anche di auto-addestramento.

Anche sul fronte processuale il legislatore ha privilegiato misure a carattere marcatamente preventivo, ritenute non rispettose della presunzione di innocenza, del principio del contraddittorio e del *ne bis in idem*[42], concentrandosi in modo particolare su una strategia di contrasto

---

no, 2015, 3-18. In materia di addestramento con finalità di terrorismo v. R. WENIN, *L'addestramento per finalità di terrorismo alla luce delle novità introdotte dal d.l. 7/2015: una riflessione comparata sulle tecniche di descrizione della fattispecie muovendo dalla sentenza del Bundesgerichtshof tedesco Str 243/13*, 2015, in *www.dirittopenalecontemporaneo.it*.

[39] Così M. DONINI, *Il diritto penale di fronte al "nemico"*, in *Cass. pen.*, 2006, 694 ss.; v. inoltre A. VALSECCHI, *La definizione di terrorismo dopo l'introduzione del nuovo art. 270-sexies c.p.*, in *Riv. it. dir. e proc. pen.*, 2006, 1097 ss.

[40] Questo è certamente il caso dell'auto-addestramento. Rilievi critici in questo senso sono stati mossi anche alla riforma spagnola dei reati di terrorismo: v. M.C. MELIÀ, *Una riforma irresponsabile, un attacco alla Costituzione*, in *www.dirittopenalecontemporaneo.it*, 2015; ID., *Il diritto penale antiterrorista spagnolo dopo la riforma del 2015*, in *Dir. pen. XXI sec.*, fasc. 2, 2015, 219-234.

[41] Così A. CAVALIERE, *Considerazioni critiche intorno al D.l. antiterrorismo n. 7 del 18 febbraio 2015*, in *Riv. trim. dir. pen. cont.*, fasc. 2, 2015, 226-235. Sul punto anche ID., *Le nuove emergenze terroristiche: il difficile rapporto tra esigenze di tutela e garanzie individuali*, in questo volume. Parimenti critico F. FASANI, *Il decreto antiterrorismo*, cit., 918 ss.

[42] E. KOSTORIS, *Il nuovo 'pacchetto' antiterrorismo, tra prevenzione, contrasto in rete e centralizzazione delle indagini*, in E. KOSTORIS, F. VIGANÒ, *op. cit.*, XV-XVIII. Per una visione organica degli strumenti di indagine utilizzabili nella lotta al terrorismo v. A. SPATARO, *Politiche della sicurezza e diritti fondamentali*, in *Terrorismo interna-*

imperniata sull'utilizzo delle nuove tecnologie. Basti pensare alla possibilità di autorizzare intercettazioni preventive al fine di acquisire notizie per la prevenzione dei delitti di cui all'art. 51, co. 3-*quater* c.p.p., se commessi mediante impiego di tecnologie informatiche o telematiche; all'obbligo in capo ai fornitori di connettività, su richiesta dell'autorità giudiziaria, di inibire l'accesso a determinati siti-internet oppure di rimuovere dalla rete contenuti di matrice terroristica; alla predisposizione di una *black list* di siti usati a fini di propaganda, reclutamento o istigazione[43].

Tale nuovo microsistema di contrasto al terrorismo, dunque, non può che affidare al potere giudiziario un compito di grande responsabilità, finalizzato al controllo sul rispetto della proporzionalità dell'intervento normativo e applicativo, da svolgere avvalendosi anche dei principi già enucleati dalle due Corti europee[44] nel dialogo mulitilivello per la tutela dei diritti[45].

## *3. Luci ed ombre del progetto di direttiva per il contrasto al terrorismo*

Avvalendosi delle prerogative attribuitegli dal Trattato di Lisbona, ed in particolare dall'art. 83 TFUE, l'Unione europea mostra la volontà di investire energie e risorse sulla armonizzazione della legislazione penale nei settori di criminalità grave e transnazionale, con l'intento di agevolare la cooperazione giudiziaria tra Stati sia in fase investigativa,

---

*zionale, politiche della sicurezza, diritti fondamentali*, in *Gli speciali di Questione Giustizia*, 2016, 167-222.

[43] Per un approfondimento v. S. SIGNORATO, *Le misure di contrasto in rete al terrorismo: black list, inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio internet*, in E. KOSTORIS, F. VIGANÒ, *op. cit.*, 56-74.

[44] Per un approfondimento v. V. SCALIA, *Controllo giurisdizionale su necessità e proporzione delle scelte di criminalizzazione del legislatore europeo: uno sguardo sulle possibilità di dialogo tra le Corti europee*, in G. GRASSO et al. (a cura di), *Le sfide dell'attuazione di una Procura europea: definizioni di regole comuni e loro impatto sugli ordinamenti interni*, Milano, 2013, 343-383.

[45] Cfr. in particolare M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione. Dal codice delle indagini preliminari a quello postdibattimentale*, in *Gli speciali di Questione Giustizia*, cit., 122 ss.

sia in vista del mutuo riconoscimento delle decisioni giudiziarie, così come previsto dall'art. 82 TFUE. L'intensa fase di sviluppo della politica criminale europea nel settore del terrorismo ha portato all'approvazione di una proposta di direttiva[46], ora al vaglio degli Stati membri, che dimostra di voler attuare una strategia basata sul paradigma di *Law Enforcement*. Essa si pone quindi in linea con quanto già previsto dai due programmi quadriennali di azione, formulati dal Consiglio europeo, il c.d. programma di Stoccolma e quello di Ypres[47], nonché dalla Comunicazione della Commissione relativa alla Agenda europea sulla sicurezza 2015[48], e chiarisce che sicurezza e diritti fondamentali devono essere intesi quali obiettivi coerenti e complementari della politica dell'Unione[49].

Leggendo più attentamente il *draft* della direttiva per il contrasto al terrorismo trasmesso agli Stati membri già alla fine del 2015, tuttavia, si nota come le reali potenzialità dell'intervento sovranazionale siano state di molto ridotte, a causa dell'appiattimento dell'articolato su quanto già previsto nella decisione quadro 2002/475/GAI, che essa sarebbe destinata a sostituire.

A causa dell'urgenza dell'intervento di armonizzazione, i principi di sussidiarietà e di proporzionalità europei, di cui all'art. 5 TUE e relativo Protocollo applicativo (n. 2 allegato al TFUE)[50], non paiono essere stati

[46] Vedi COM(2015) 625 final, *Proposal for a Directive on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism*, reperibile on-line: *www.ec.europa.eu*.

[47] Il programma di Stoccolma per il quadriennio 2010-2014 è reperibile on-line: *http://eur-lex.europa.eu*; per il programma di Ypres vedi la pagina ufficiale del Consiglio europeo, *http://www.consilium.europa.eu*.

[48] COM(2015), Strasbourg, 28 April 2015, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, on-line: *www.ec.europa.eu*.

[49] Nell'*explanatory memorandum* si precisa: "Security and respect for fundamental rights are not conflicting aims, but consistent and complementary policy objectives" (cfr. *Fundamental Rights*, p. 13 del *draft*).

[50] Per un approfondimento sul principio di sussidiarietà, tra la sterminata letteratura, basti il rinvio A. BERNARDI, *I principi di sussidiarietà e di legalità nel diritto penale europeo*, in *Riv. trim. dir. pen. econ.*, 2012, 15 ss.; ID., *La competenza penale accessoria dell'Unione europea: problemi e prospettive*, on-line: *www.penalecontemporaneo.it*. Più ampiamente, anche per gli opportuni riferimenti bibliografici, v. G. GRASSO, *La*

rispettati, visto che le scelte punitive possono ascriversi più ad obblighi di matrice internazionale che a consapevoli valutazioni e decisioni assunte in sede europea. L'*Explanatory memorandum*, che accompagna il progetto, nella sezione rubricata *subsidiarity*, infatti, riporta una laconica giustificazione circa l'opportunità di intervenire a livello sovranazionale e fa uno stringato richiamo agli strumenti internazionali vincolanti per gli Stati, quale fondamento (quasi obbligato) delle scelte di politica criminale effettuate che, in tal modo, non possono che essere in linea con gli adeguamenti normativi già implementati a livello nazionale. Gli autori del *draft* sottolineano inoltre che, avendo aderito al Protocollo addizionale del Consiglio d'Europa del 22 ottobre 2015, secondo la procedura di cui all'art. 218 TFUE, l'Unione risulta altresì vincolata ad adottare incriminazioni minime aderenti alle indicazioni fornite in tale ultimo strumento per adeguare la risposta ai mutamenti del fenomeno ed evitare lacune di tutela o frammentazione della disciplina di contrasto, che metterebbero a rischio la sicurezza degli Stati membri e dei cittadini.

In ordine al principio di proporzionalità, la giustificazione si fa ancora più scarna. Il legislatore europeo, infatti, riporta solo una dichiarazione tautologica, tale per cui il contenuto della direttiva si limita a ciò che è necessario e proporzionato da un lato per l'implementazione degli obblighi e degli standard stabiliti a livello internazionale e, dall'altro lato, per adeguare le fattispecie penali già in vigore alla nuova minaccia terroristica.

Considerato inoltre che, in ragione dell'urgenza di modificare l'assetto legislativo per il contrasto al terrorismo e di aumentare il grado di sicurezza a fronte dei recenti attacchi terroristici, il *draft* della direttiva è stato eccezionalmente approvato senza il preliminare *impact assess-*

*«competenza penale» della Unione europea nel quadro del Trattato di Lisbona*, in G. GRASSO, L. PICOTTI, R. SICURELLA (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, 683 ss.; v. anche R. SICURELLA, *«Prove tecniche» per una metodologia dell'esercizio delle nuove competenze concorrenti dell'Unione europea in materia penale*, *ivi*, 3 ss.

*ment*[51], si può concludere affermando che anche l'Unione europea ha ceduto di fronte alle spinte emergenziali.

Guardando al merito della direttiva, si nota la preferenza per formulazioni generiche degli obblighi di incriminazione che lasciano agli Stati adeguati spazi di manovra per la delineazione del precetto e per la determinazione della soglia di offensività della condotta da implementare. Tale genericità, inoltre, permette ai Parlamenti nazionali di valutare l'opportunità di intervenire sul proprio sistema nazionale, visto che ormai tutti gli ordinamenti sono muniti di una propria disciplina antiterrorismo, quantomeno per la punibilità dei reati di direzione e partecipazione ad un gruppo terroristico, di cui all'art. 4 della direttiva, di istigazione a commettere reati di terrorismo previsto dal successivo art. 5, di arruolamento ed addestramento con finalità di terrorismo, artt. 6 e 8 e di finanziamento del terrorismo ex art. 11 del *draft*.

Per questi motivi non paiono potersi condividere le preoccupazioni sollevate da alcune associazioni internazionali per la tutela dei diritti umani rispetto al testo della direttiva, in relazione all'eccessiva anticipazione di tutela, alla violazione del principio di determinatezza, alla inidoneità dell'elemento soggettivo a selezionare condotte concretamente offensive del bene protetto, nonché alla mancanza di limiti idonei ad arginare interventi punitivi sproporzionati[52]. Infatti, sarà onere

[51] Vedi il documento predisposto dalla Commissione europea, *Guidelines on Impact Assessment*, che enucleano le fasi principali da seguire per valutare l'efficienza, in termini anche di sussidiarietà, delle nuove iniziative legislative e non dell'Unione. Online: *www.ec.europa.eu*.

[52] Cfr. il *report* dal titolo "European Commission's proposal for a Directive of the European Parliament and of the Council on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA on Combating Terrorism", del febbraio 2016. Le problematiche appena evidenziate non sono invece state colte dal Senato della Repubblica italiana che, in sede di relazione alla proposta di direttiva sulla lotta al terrorismo, non ha rilevato alcuna criticità né in merito al rispetto dei principi di sussidiarietà e proporzionalità, né rispetto alla formulazione degli obblighi di incriminazione inseriti nel *draft*. Cfr. Nota n. 37 su atti dell'Unione europea, dd. 18.02.2016, dal titolo: "Proposta di direttiva del Parlamento europeo e del Consiglio sulla lotta contro il terrorismo e che sostituisce la decisione quadro del Consiglio 2002/475/GAI sulla lotta contro il terrorismo" emessa a seguito dell'inoltro della relazione a cura della Presidenza del Consiglio dei Ministri, Dipartimento Politiche Europee dd. 10.02.2016, reperibili online su *www.senato.it*.

degli Stati membri precisare i singoli elementi costitutivi delle fattispecie, coordinandole con le previsioni nazionali, nonché stabilire i rigorosi limiti entro cui sarà possibile comprimere le libertà dei cittadini ed i relativi rimedi in caso di violazione.

Infatti, la scelta di prevedere delle fattispecie a forte vocazione preventiva, non può essere automaticamente delegittimata e il suo risultato accostato in modo acritico al ben noto "diritto penale del nemico" di jakobsiana memoria[53]. Non a caso attenta dottrina ha coniato il termine di «diritto penale al limite»[54], ovvero un diritto penale che

> si muove in un'area dove è sempre alto il rischio che la ragionevolezza delle scelte di incriminazione, delle strategie processuali e delle misure preventive si traduca in forme illegittime di violazione di diritti e libertà fondamentali[55].

Ciò che si può e si deve rimproverare al legislatore sovranazionale, oltre al fatto di aver innovato la disciplina europea di contrasto al terrorismo nella forma e non nella sostanza, è l'assenza di una apposita sezione dedicata alla cooperazione giudiziaria e, in particolare, all'implementazione e regolamentazione di strumenti investigativi a contenuto tecnologico, anche di natura proattiva, finalizzati al controllo di siti web, piattaforme social o comunque di flussi di comunicazioni scambiate a mezzo Internet. Tale lacuna pare ancora più grave se si pensa che ancora oggi, a seguito della invalidazione ad opera della Corte di giustizia della direttiva 2006/24/CE[56], avvenuta nel 2014, risulta mancare una disciplina in materia di conservazione dei dati di traffico a fini

[53] Per un approfondimento: v. G. JAKOBS, *Diritto penale del nemico*, in M. DONINI, M. PAPA (a cura di), *Diritto penale del nemico. Un dibattito internazionale*, Milano, 2007, 5 ss.; ID., *Diritto penale del nemico?*, in A. GAMBERINI, R. ORLANDI (a cura di), *Delitto politico e diritto penale del nemico*, Bologna, 2007, 109 ss.

[54] Così M. PELISSERO, *Contrasto al terrorismo internazionale e diritto penale al limite*, in *Gli speciali di Questione Giustizia*, cit., 2016, 99-122.

[55] *Ibid.*, 101.

[56] Per un approfondimento: v. R. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Riv. trim. dir. pen. cont.*, 2014, fasc. 2, 178-190.

di indagine, con ovvie ripercussioni anche sui diritti degli indagati e dei cittadini in generale[57].

## *4. Conclusioni: verso un nuovo paradigma extra-sistemico della sicurezza?*

Non si può che concludere con l'auspicio che l'articolato del *draft* della nuova direttiva venga nuovamente rivisto ed integrato, al fine di creare uno strumento completo e realmente efficacie per il contrasto transnazionale al fenomeno. Allo stesso modo, vista l'obiettiva tendenza degli Stati membri a conferire sempre maggiori poteri ai servizi segreti[58], sarebbe opportuno un intervento da parte del legislatore europeo nel settore, al fine di creare non solo una struttura accentrata di riferimento, che possa interloquire con gli agenti degli Stati terzi, ma soprattutto una base normativa condivisa che possa stabilire i limiti di ricerca di informazioni in Internet e la loro eventuale (e forse non auspicabile) utilizzabilità all'interno dei procedimenti penali e amministrativi degli Stati membri, ove peraltro già ci si è avvalsi di prove segretate per ragioni di sicurezza nazionale[59].

In Italia, ad esempio, destano preoccupazioni le modifiche introdotte dal d.l. n. 7/2015 alla legge n. 124/2007, che regola l'attività dei servizi di *intelligence*[60]. Sul versante sostanziale, la lett. a) del comma 2 del-

[57] Sul punto: v. M. DANIELE, *Le indagini informatiche contro il terrorismo. Bilanciamenti difficili e timori legislativi*; F. IOVENE, *Contrasto al terrorismo, indagini informatiche e tutela dei diritti fondamentali*, in questo volume.

[58] Vedi le già richiamate modifiche introdotte in Francia dalla Loi n. 2015-912, approvata il 24 giugno 2015 e in Gran Bretagna grazie all'emendamento al *Computer Misuse Act*, introdotto dal *Serious Crime Act 2015*, approvato il 3 marzo 2015, nonché alle modifiche alla legge 124/2007, introdotte in Italia dall'art. 8 della legge n. 43/2015.

[59] Vedi, *inter alia*, i rilievi della Corte di giustizia nella causa C-300/11, *ZZ / Secretary of State for the Home Department*.

[60] Per un commento più ampio v. V. MEZZOLLA, *Ampiamento delle garanzie funzionali e di tutela processuale del personale e delle strutture di servizi di informazione per la sicurezza*, Commento al d.l. 7/2015, art. 8, in *www.legislazionepenale.eu*, 2016.

l'art. 8, in vigore fino al 31 gennaio 2018[61], infatti, amplia l'ambito di operatività delle garanzie funzionali di cui all'art. 17 della stessa legge, oggi applicabili (oltre che ai già previsti reati di cui agli artt. 270-bis co. 2 e 416-bis) anche ai reati di cui agli artt. 270 co. 2, 270-*ter*, 270-*quater*, 270-*quater.1*, 270-*quinquies*, 302, 306 co. 2 e 414 co. 4 c.p. L'effetto di tale modifica è quello di permettere allo Stato di opporre una causa di giustificazione a favore del personale dei servizi di informazione per la sicurezza (appartenenti sia all'AISE sia all'AISI)[62] in tutti i casi in cui questi ultimi, nell'esercizio delle proprie funzioni, si trovino a porre in essere condotte costituenti reato, previamente autorizzate ai sensi dell'art. 18 della legge 124/2007.

Tale scriminante, operando in un settore tipicamente di prevenzione, slegato dall'attività di polizia giudiziaria[63], potrebbe creare distorsioni rispetto ai principi fondanti il giusto processo, aumentando i rischi di impunità rispetto a condotte obiettivamente illecite. Essa, inoltre, assume un carattere politico e per questo difficilmente sindacabile, posto che si basa su una autorizzazione di natura procedurale, la cui valutazione circa i presupposti applicativi – tra cui la proporzionalità dell'azione rispetto agli obiettivi da perseguire, il grado di invasività rispetto ai diritti coinvolti, nonché la correttezza del bilanciamento tra interessi pubblici e privati operato – è demandata al Presidente del Consiglio dei Ministri (o l'autorità da lui delegata).

L'autorità giudiziaria viene così relegata ad un ruolo meramente marginale e spogliata della sua vocazione alla tutela dei diritti: nel caso in cui si instaurasse un processo, il giudice dovrebbe prendere atto della sussistenza di un provvedimento di autorizzazione e, nell'eventualità in cui nutrisse dubbi sulla sussistenza dei presupposti per il rilascio, po-

[61] Pare opportuno precisare che siffatta limitazione temporale vale solo per le previsioni in materia di garanzie funzionali e non invece per quelle relative all'utilizzo dell'identità di copertura nel processo penale.

[62] Le competenze di AISE (agenzia per l'informazione e la sicurezza esterna) ed AISI (agenzia per l'informazione la sicurezza interna) sono elencate rispettivamente negli articoli 6 e 7 della Legge 124/2007.

[63] Per un approfondimento vedasi G. AMATO, *Garanzie funzionali più ampie a chi è sotto copertura*, in *GD*, fasc. 11, 2015, 92 ss.

trebbe unicamente sollevare un conflitto di attribuzione davanti alla Corte costituzionale[64].

All'estensione delle scriminanti funzionali si aggiunge anche quanto previsto dal comma 2-bis dell'art. 8 d.l. 7/2015, che dispone che sia

> affidato all'AISE il compito di svolgere attività di informazione, anche mediante assetti di ricerca elettronica, esclusivamente verso l'estero, a protezione degli interessi politici, militari, economici, scientifici e industriali della Repubblica italiana.

Si percepisce così l'effetto dirompente della disposizione in materia di indagini ad alto contenuto tecnologico, vista la legittimazione riconosciuta alle c.d. *bulk interceptions*[65].

Per quanto si condivida la necessità di un rafforzamento delle attività di natura preventiva, soprattutto a fronte dell'utilizzo ormai massivo di Internet a fini di propaganda, di reclutamento, oltre che come strumento per sferrare attacchi di matrice terroristica ad infrastrutture sensibili[66], sembra imprescindibile, in futuro, riflettere sulle modalità di coordinamento tra *intelligence* e indagini penali. Discussioni in merito alla utilizzabilità – o alla opportunità di rendere utilizzabili – "prove di *intelligence*" nei procedimenti penali, essendo già state affrontate in seno al Comitato antiterrorismo del Consiglio di Sicurezza[67], non sarebbero certo nuove nello scenario internazionale.

---

[64] Sul punto si rinvia alle considerazioni svolte da P. PISA, *Le garanzie funzionali per gli appartenenti ai Servizi segreti*, in *Dir. pen. proc.*, 2007, 1431 ss.

[65] Per un approfondimento in materia di *strategic surveillance*, legato ai meccanismi di aggiramento delle garanzie stabilite a livello nazionale per la tutela della riservatezza dei cittadini e alla difficoltà di individuare i selettori corretti, al fine di filtrare l'ampia mole di dati acquisiti cfr. *European Commission for Democracy through Law (Venice Commission), Study no. 719/2013*, adottato il 20-21 marzo 2015, dal titolo "Update of the 2007 Report on Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signal Intelligence Agencies".

[66] Per un approfondimento: v. R. FLOR, *Il contrasto al terrorismo nell'era delle nuove tecnologie e i meccanismi di cooperazione fra settore pubblico e settore privato*, cit., 513-546.

[67] Per un approfondimento: v. *Directorate General for Internal Policies, Policy Department C: Citizens's Rights and Constitution Affairs, Justice Freedom and Security,*

L'argomento è senz'altro delicato: l'avvicinamento dei servizi alle attività della polizia giudiziaria rischia di fornire una delega in bianco al potere esecutivo, affinché possa operare a tutela della Ragion di Stato slegato dai rigorosi limiti dell'ordinamento, attraverso l'esercizio di facoltà destinate a travalicare i limiti segnati dalla stessa tripartizione dei poteri.

Si andrebbe così a creare un terzo paradigma della sicurezza, diverso rispetto a quello bellico ed a quello basato sul *Law Enforcement*, poiché extra-sistemico e figlio dello stato di eccezione[68].

Esso sarebbe paragonabile al c.d. *Extra Legal Measures Model*[69], formulato in sede di teorizzazione delle possibili reazioni dello Stato di fronte all'emergenza, che concede all'esecutivo la facoltà di agire *extra ordinem*, con il fine ultimo di preservare l'integrità del sistema giuridico, evitando modifiche (di lungo o breve periodo) e sospensioni di garanzie costituzionali.

Tale modello, a seguito dell'atto di disobbedienza, richiederebbe comunque di rendere edotta l'opinione pubblica di tutti i dettagli dell'azione necessitata, affinché essa, a mezzo dei suoi delegati, possa procedere all'approvazione di un *Act of Indemnity* (la cui forma sarebbe rimessa alla discrezionalità dello Stato), oppure alla condanna delle pubbliche autorità per aver abusato dei poteri straordinari connessi all'eccezione che hanno ritenuto di dover istituire[70].

Purtroppo, una simile teoria non troverebbe grande fortuna nella prassi: al di là della sottrazione delle decisioni politiche al vaglio delle Corti, l'esperienza ha dimostrato come l'esecutivo sia incline, anche

---

*study "National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges"*, 2014, on-line: *http://www.europarl.europa.eu/*.

[68] Sul punto v. G. AGAMBEN, *Stato di eccezione*, Torino, 2010; R. BARTOLI, *Regola ed eccezione nel contrasto al terrorismo internazionale*, in M. MECCARELLI, P. PALCHETTI, C. SOTIS (a cura di), *Le regole dell'eccezione: un dialogo interdisciplinare a partire dalla questione del terrorismo*, Macerata, 2011, 170 ss.

[69] Per gli opportuni approfondimenti e riferimenti bibliografici: v. O. GROSS, F. Ní AOLÁIN, *Law in Times of Crises. Emergency Powers in Theory and Practice*, Cambridge, 109 ss.; O. GROSS, *Stability and Flexibility: a Dicey Business*, in V. RAMRAJ, M. HOR, K. ROACH (eds.), *Global Anti-Terrorism Law and Policy*, Cambridge, 2005, 90 ss.

[70] Cfr. O. GROSS, F. Ní AOLÁIN, *Law in Times of Crises*, cit., 112 ss.

secondo presupposti criticabili, all'utilizzo del segreto di stato e delle immunità funzionali legate alle esigenze di salvezza dello Stato e dei suoi interessi latamente intesi, quale schermatura rispetto ad azioni assunte in contrasto con quanto prescritto dall'ordinamento e con i livelli minimi di tutela delle libertà fondamentali[71].

[71] Vedi per l'Italia la nota vicenda di Abu Omar in relazione alla partecipazione dei servizi italiani nell'attività di *extraordinary rendition*. In particolare le considerazioni di R. ORLANDI, *Una pervicace difesa del segreto di Stato*, in *Giur. cost.*, 2012, 2327 ss.; M. PANZAVOLTA, *La Corte Costituzionale e la cortina del segreto (dell'imputato) sull'accusa di attività "deviata" dei servizi segreti*, in *Cass. pen.*, 2012, 3275 ss.; per una panoramica generale v. R. VAN ALEBEEK, *The Immunity of States and their Officials in International Criminal Law and International Human Rights Law*, Oxford, 2008.

SECONDA SESSIONE

# IL DIRITTO PENALE NELL'ERA DEL TERRORISMO GLOBALIZZATO, OVVERO IL DELICATO BILANCIAMENTO TRA ESIGENZE DI CONTRASTO E LA TUTELA DEI DIRITTI FONDAMENTALI

*Beniamino Migliucci*

Desidero, prima di tutto, ringraziare il Prof. Fornasari e il Dott. Roberto Wenin per avermi invitato a questo importante convegno organizzato dall'Università di Trento.

Nell'era del terrorismo globalizzato – che rispetto a fenomeni equipollenti del passato, proprio a causa del mutare repentino della società contemporanea, appare più impalpabile e sfuggente – affrontare temi come la sicurezza, il diritto penale del nemico, l'emergenza, la sospensione dei diritti e delle garanzie fondamentali dei cittadini, l'estensione degli strumenti di contrasto ai fenomeni terroristici anche a ipotesi di reato che nulla hanno a che vedere con gli stessi, è compito arduo e delicato, perché la paura che tali fenomeni insidiosamente instillano nella società moderna – complice, forse, anche la velocità e la liquidità con cui, attraverso il *web*, circolano le informazioni – rischia di far perdere di vista ai Legislatori nazionali e sovranazionali, nonché all'uomo della strada, l'importanza del ruolo e la centralità di alcuni principi cardine che connotano le democrazie contemporanee in generale, e i rispettivi ordinamenti penali in particolare, ovvero il principio di legalità, di determinatezza e tassatività della fattispecie, di irretroattività della legge penale, del giusto processo di cui all'art. 111 della Costituzione.

Sembra che questi principi fondamentali perdano di importanza e si sbiadiscano di fronte al bisogno di sicurezza e alla necessità di contrastare fenomeni nuovi e difficilmente prevedibili.

La sicurezza è sicuramente un obiettivo da perseguire, ma questo non giustifica scelte autoritarie che non rappresentano un deterrente e pongono a rischio la solidità di una architettura in materia di politica

giudiziaria che trae la sua forza proprio dal rispetto, in qualsiasi situazione, di quei principi fondamentali.

Mi piace, dunque, ricordare le parole del Ministro della Giustizia On. Andrea Orlando che, in occasione delle comunicazioni del Guardasigilli sull'amministrazione della giustizia a gennaio 2016, innanzi alla Camera dei Deputati, ha avuto modo di rammentare come

> il terrorismo, anche quello jihadista, ha caratteristiche originali. La cooperazione tra Stati è indispensabile in un periodo in cui il terrore vorrebbe mettere alla prova lo Stato di diritto, che invece deve uscirne più forte. L'impegno contro il terrorismo non deve significare cedere un solo millimetro sul terreno dei principi costituzionali da cui dipende il fitto tessuto di libertà che informano la nostra democrazia

che, aggiungo, va difesa non solo dal terrorismo, ma anche da quelle tentazioni autoritarie che vorrebbero colpire indistintamente tutti.

«Non possiamo e non vogliamo smettere», ha affermato ancora il Ministro, di essere

> quella regione del mondo in cui è più profondo e radicato il riconoscimento dei diritti dell'uomo. Essere europei significa considerare questo spazio di libertà e di uguaglianza come la propria casa. Le generazioni che ci hanno consegnato quest'eredità non possono essere tradite, e anzi è nostro dovere arricchire questo sistema di diritti e garanzie.

Queste parole, in un momento storico così intenso e drammatico, in cui il terrorismo di matrice islamista ha segnato il mondo intero, costituiscono un monito e una sfida importante, sia per l'Italia che per l'Unione europea, spazio di libertà e giustizia, che non possono cedere al ricatto della paura attraverso atteggiamenti ondivaghi e la compressione delle garanzie dei cittadini, di cui va, in ogni caso, garantita la sicurezza.

Nello stesso solco delle considerazioni svolte dal Ministro della Giustizia, si collocano le parole dell'allora primo Presidente della Suprema Corte di Cassazione, Dott. Giovanni Canzio, pronunciate in occasione dell'inaugurazione dell'anno giudiziario 2016, il quale ha ricordato come

> l'azione di contrasto verso ogni forma organizzata di criminalità anche terroristica internazionale deve avvenire nelle regole stabilite dalla Costituzione e dalle leggi dello Stato. Diversamente tradiremmo la memoria di quanti sono caduti in difesa dei più alti valori democratici e non faremmo onore al giuramento di fedeltà che abbiamo prestato.

Lo Stato di Diritto, modello attraverso cui abbiamo plasmato le democrazie contemporanee, è e deve rimanere la cornice nell'ambito della quale si devono bilanciare le esigenze di sicurezza con la tutela dei diritti fondamentali delle persone.

Bisogna, dunque, rifuggire non solo qualsiasi allarme emergenziale, fenomeno costante soprattutto nella storia della politica criminale del nostro Paese, ma anche, e soprattutto, ogni tentazione autoritaria volta all'introduzione di modelli paralleli (o doppi binari) che, come specchietti per le allodole, con la scusa di rappresentare e offrire un sistema in grado di garantire maggiore sicurezza, altro non fanno se non contraddire i principi cardine dello Stato di Diritto, minandoli nelle proprie fondamenta.

Porre l'esigenza di sicurezza su di un piano superiore, mettere la stessa al centro dell'ordinamento giuridico, non porterebbe ad altro se non alla relativizzazione o, peggio ancora, all'affievolimento dei diritti fondamentali.

In questa prospettiva, qualsiasi inversione di tendenza dell'ordinamento penale verso prospettive emergenziali e di necessità di maggiore sicurezza costituirebbe essa stessa una gravissima violazione dei diritti umani fondamentali, riconosciuti non solo dalla nostra Costituzione, ma anche dalla Dichiarazione Universale dei Diritti dell'Uomo del 1948 e dalla Convenzione Europea dei Diritti dell'Uomo del 1950.

Rammenta Roberto Wenin come spesso l'emergenza e il bisogno di sicurezza portano il Legislatore a violare i canoni della determinatezza della fattispecie, anticipando in modo irragionevole anche la soglia della punibilità, il che, nella sua massima declinazione, potrebbe portare a presunzioni di pericolosità e a un modello di diritto penale d'autore.

In un momento in cui si criticano persino pronunce della Corte Europea dei Diritti dell'Uomo quando ritenute troppo ispirate alle garanzie della persona, è necessario considerare la differenza tra le diverse tradizioni giuridiche degli Stati membri dell'Unione europea, al fine di ar-

monizzare la normativa europea al sistema dei valori e principi costituzionali propri di ciascun Paese. Ciò non significa essere diffidenti rispetto alla complessità del sistema sovranazionale di cui facciamo parte, e che vorremmo essere ricco di libertà, ma occorre prendere reciprocamente atto delle specificità e delle peculiarità di ciascun sistema, tenendo conto, nel nostro caso, dei principi e dei valori irrinunciabili espressi dalla nostra Costituzione.

Alla luce delle sfide che il terrorismo ci impone, si devono contemperare, dunque, principi, valori ed esigenze, che anche i decreti legislativi del febbraio 2016 in materia di lotta al terrorismo, nelle premesse e nel preambolo, sembrano condividere e rispettare.

Vi si legge, in particolare, che le disposizioni non devono essere incompatibili con i principi dell'ordinamento costituzionale in tema di diritti fondamentali, di diritti di libertà e del giusto processo, il che sembra coerente alla prospettiva di bilanciare le "esigenze dei diritti fondamentali" con le esigenze di sicurezza.

La capacità di rimanere fedeli alla nostra tradizione, alla nostra cultura giuridica, la corretta applicazione delle norme di recente approvate costituirà un banco di prova importante per dimostrare che la paura non riesce a scalfire la stabilità delle democrazie avanzate.

# DA AL QAEDA ALL'ISIS: LA SECONDA FASE DEL TERRORISMO ISLAMISTA. STRUMENTI GIURIDICI, PRIME APPLICAZIONI E RIFLESSIONI CULTURALI[1]

*Guido Salvini*

SOMMARIO: *1. In ricordo delle vittime italiane del terrorismo islamico. 2. Le norme di contrasto al terrorismo internazionale dopo gli attentati di New York. 3. Arruolamento e* foreign fighters*: l'intervento legislativo del febbraio 2015. 4. Approcci giurisprudenziali e prime applicazioni. 5. Qualche riflessione culturale.*

## *1. In ricordo delle vittime italiane del terrorismo islamico*

Prima di affrontare il tema del terrorismo internazionale nella sua fase attuale sembra necessario ricordare e parlare delle vittime italiane di tale forma di terrorismo.

Sono cittadini italiani caduti all'estero, per la maggior parte completamente dimenticati forse perché rimangono soggetti sparsi che non rappresentano un gruppo sociale riconoscibile che è possibile ricordare in uno specifico territorio come le vittime delle stragi eversive degli anni '70.

Senza tornare indietro nel tempo sino alle due stragi di Fiumicino nel dicembre 1973 e nel dicembre 1985[2] e all'abbattimento 19 settembre 1989 nel deserto del Tenerè di un DC 10[3] da parte dei libici e individuando come momento di partenza l'attentato alle Torri Gemelle del 2001 va ricordato che le vittime civili italiane degli ultimi anni sono

[1] Testo aggiornato ed ampliato dall'intervento per il convegno *Diritto penale e modernità*, Trento, 2-3 ottobre 2015.

[2] Rispettivamente del 17 dicembre 1973 e del 27 dicembre 1985, con complessive 65 vittime di cui otto italiane.

[3] A bordo del quale si trovavano 170 passeggeri di cui dieci cittadini italiani.

ormai circa 40[4]. In Iraq, Afghanistan, Arabia Saudita, Egitto, Nigeria, Turchia, Bangladesh sono morti in attentati tecnici, cooperanti, lavoratori in alberghi, semplici turisti tra i quali i quattro turisti morti nell'attentato al museo del Bardo in Tunisia di cui non si ricordano nemmeno i nomi. Tra le ultime vittime Cesare Tavella, cooperante in Bangladesh, ucciso nel settembre 2015, probabilmente la prima vittima italiana rivendicata dall'ISIS, Valeria Solesin uccisa nell'attentato al teatro Bataclan di Parigi il 13 novembre 2015 e Fabrizia Di Lorenzo uccisa il 19 dicembre 2016 nell'attentato al mercatino di Natale di Berlino.

Poi in crescendo la strage al ristorante di Dacca, quella in cui sono morti contemporaneamente più cittadini italiani, uccisi insieme ad altri cittadini stranieri che non sapevano recitare versetti del Corano, a colpi di coltello e di altre armi da taglio da un commando dell'ISIS[5].

E infine i sei cittadini italiani vittime della strage sul lungomare di Nizza il 14 luglio 2016.

Senza dimenticare i numerosi tecnici e giornalisti rapiti e spesso rilasciati dopo molti mesi e senza dimenticare, per altro verso, Giulio Regeni, vittima di una violenza con ogni probabilità interna alle istituzioni o a fazioni delle istituzioni del regime egiziano, con i conseguenti "depistaggi" delle indagini che sinistramente ricordano i depistaggi dei Servizi di sicurezza del nostro paese nelle indagini sulle stragi eversive degli anni '70, da piazza Fontana in poi.

Sinora cittadini italiani sono caduti vittime di attentati solo in territori esteri. All'interno nel nostro paese non si sono registrate azioni significative se non quella di un "lupo solitario" libico che il 12 ottobre 2009 ha collocato un ordigno artigianale a Milano in una caserma dell'esercito peraltro ferendo gravemente solo se stesso[6]. La ragione di questa

[4] Per un elenco aggiornato delle vittime italiane del terrorismo internazionale si veda il sito *http://vittimeterrorismo.it/memorie/elenco_vit_int.html*.

[5] La morte inferta agli ostaggi con coltelli, anche quando sarebbe possibile ucciderli più velocemente con armi da fuoco, ha un valore rituale. Con armi da taglio vengono uccisi gli animali domestici e ciò sta a significare che gli infedeli, destinati alla dannazione, non sono degni nemmeno di essere collocati al rango di essere umani.

[6] L'attentatore Mohamed Game si era addestrato al confezionamento di ordigni via Internet ed era stato aiutato da due complici che tuttavia, come lui, non appartenevano ad alcuna organizzazione.

immunità origina dal fatto che sin dall'inizio degli anni 2000 l'Italia ha continuato ad essere considerata più una base logistica e di rifugio che un obiettivo. D'altronde essa è il principale punto di approdo dei migranti che vengono dal Nord Africa, attività che fornisce proventi anche ad organizzazioni islamiche, soprattutto in Libia, e quindi sarebbe una cattiva strategia compiere una grande azione in Italia con il rischio di provocare una reazione di blocco dell'immigrazione. Certo il pericolo resta sensibile in quanto è vero che il nostro paese è considerato una potenza occidentale di seconda classe ma nel contempo esso è anche la sede del Vaticano che è in sostanza, come centro di irradiazione della cristianità, l'obiettivo finale dell'islamismo politico[7] e quindi non è consentito formulare una prognosi, come si dice favorevole.

## *2. Le norme di contrasto al terrorismo internazionale dopo gli attentati di New York*

Dopo questo ricordo, non solo "tecnico" ma doveroso sul piano civile, sembra utile, per disporre subito di un quadro di sintesi, ricordare che la legislazione interna in materia di terrorismo internazionale può suddividersi in quattro fasi che corrispondono alla nascita e all'evolversi del fenomeno: la fase precedente e immediatamente successiva all'attentato alle Torri Gemelle, quella successiva ai gravi attentati alla stazione ferroviaria Atocha di Madrid nel 2004 e alla metropolitana di Londra nel 2005 e infine la fase attuale segnata soprattutto dal terrorismo dell'ISIS e dalla nascita dello Stato islamico.

Queste in sintesi sono state le risposte del legislatore:

- sino al 2001, nella fase di incubazione del terrorismo internazionale era stato possibile applicare a soggetti individuati in Italia solo le norme "ordinarie" quali l'associazione per delinquere e quelle relative ai reati strumentali come la falsificazione o la ricettazione di documenti. Infatti non esisteva alcuna norma che consentisse di riconoscere la "finalità il terrorismo", normalmente applicata nei con-

[7] In numerose immagini diffuse via Internet dall'Isis sono rappresentati con fotomontaggi combattenti islamici armati che alzano la loro bandiera nera sui palazzi del Vaticano.

fronti delle organizzazioni terroristiche interne, quando l'obiettivo fosse esclusivamente uno Stato o una istituzione estera. Erano comparse negli anni '90 in Italia alcune cellule del GIA (Gruppo Islamico Algerino) ma si trattava di gruppi che utilizzavano l'Italia solo come retrovia e l'obiettivo restava quello di colpire esclusivamente obiettivi algerini. Quindi nei loro confronti, conclusione cui erano giunte tutte le sentenze, non era applicabile la finalità di terrorismo e tutte le norme collegate[8].

- subito dopo l'attacco alle Torri Gemelle e con grande tempestività il Decreto legge 18 ottobre 2001 n. 374[9] aveva modificato l'art. 270-*bis* Codice penale introducendo un terzo comma secondo cui «la finalità di terrorismo ricorre anche quando gli atti di violenza sono rivolti contro uno Stato estero, un'istituzione e un organismo internazionale»[10]. Si è aggiunta altresì nell'art. 270-*bis* per la prima volta la

[8] Sulla inapplicabilità nei confronti delle prime cellule, soprattutto algerine, radicatesi in Italia ma con obiettivi comunque diretti contro il proprio paese d'origine del reato associativo cui all'art. 270-*bis* Codice penale e dell'aggravante della finalità di terrorismo si veda, tra le molte, Cass. Sez. VI, 1 giugno 1999 in *Dir. e proc. pen.*, 1999, 966 e, in un caso singolare che vedeva alcuni cittadini italiani legati all'estrema destra impegnati nell'organizzare un colpo di Stato nelle isole Comore, Cass. Sez. VI, 1 luglio 2003, n. 36776, Nerozzi ed altri.

[9] Convertito con modificazioni nella legge 15 dicembre 2001 n. 438. Sull'art. 270-*bis* c.p. così come ridefinito dal legislatore nel 2001 si veda ampiamente F. ROBERTI, *Le nuove fattispecie di delitto in materia di terrorismo*, in A.A. DALIA (a cura di), *Le nuove norme di contrasto al terrorismo. Commento al Decreto-legge 27 luglio 2005, n. 144 convertito, con modificazioni, nella legge 31 luglio 2005, n. 155 ed integrato dal Decreto-legge 30 dicembre 2005, n. 272, convertito, con modificazioni, nella legge 21 febbraio 2006, n. 49 e sintesi dei lavori parlamentari*, Milano, 2006, 447 e ss.

[10] Con lo stesso provvedimento, riscrivendo interamente l'art. 226 Disposizioni di attuazione al c.p.p., sono state estese ai reati con finalità di terrorismo le intercettazioni preventive delle comunicazioni o conversazioni anche per via telematica che possono essere richieste dai Servizi centrali di investigazione al Procuratore della Repubblica e comportano l'intercettazione delle comunicazioni anche se queste avvengono nei luoghi indicati dall'articolo 614 c.p. quando ciò sia necessario per l'acquisizione di notizie concernenti la prevenzione dei delitti di cui all'art. 407 comma 2 lettera a) n. 4 e 51 comma 3-*bis* c.p.p. Le intercettazioni così svolte possono essere utilizzate solo a fini investigativi e non possono fare ingresso nel procedimento penale ed è prevista la loro distruzione dopo il deposito presso la Procura della Repubblica che le ha autorizzate.

condotta di finanziamento di associazioni con finalità di terrorismo, applicabile sia in caso di terrorismo interno sia in caso di terrorismo internazionale ma pensata soprattutto per quest'ultimo.

In questo modo è stato possibile proiettare anche all'esterno gli obiettivi delle cellule che si stavano radicando in Italia, colpire i loro associati e rendere più efficace l'attività di contrasto. Negli anni successivi sono state infatti neutralizzate alcune cellule, operanti soprattutto a Milano e a Brescia, che utilizzavano il nostro paese come retrovia logistica ed inviavano denaro, documenti falsi e combattenti, i precursori dei *foreign fighters* attuali, nelle zone dell'Iraq ove Ansar al Islam e altri gruppi contrastavano con attentati l'intervento degli Stati Uniti e degli altri paesi occidentali e le strutture del nuovo governo in via di formazione dopo la caduta del presidente Saddam.

- con il decreto-legge 27 luglio 2005 n. 144, il c.d. pacchetto Pisanu, dal nome del Ministro dell'Interno dell'epoca, adottato subito dopo l'attentato alla metropolitana di Londra del 7 luglio 2005, la legislazione di contrasto del terrorismo internazionale ha compiuto un altro passo in avanti sino a configurarsi ormai come un "sottosistema" investigativo, processuale e sostanziale. Sono stati infatti inseriti nel capo relativo ai Delitti contro la personalità internazionale dello Sta-

---

Le intercettazioni preventive sono uno strumento parziale ma che può rivelarsi di utilità per monitorare l'attività di soggetti, non entrati ancora in un'indagine, in specifici contesti quali soprattutto gli istituti carcerari ove si trovino molti detenuti musulmani e ove vi siano segnali di indottrinamento. Infatti i carceri, più ancora delle moschee e dei Centri culturali islamici sono un terreno fertile per il reclutamento di giovani musulmani legati a piccole attività criminose e privi di qualsiasi punto di riferimento. Ciò in ragione soprattutto del fatto che in molte carceri, come più volte segnalato anche dal Ministro dell'Interno, tali detenuti tendono a raggrupparsi intorno ad *Imam* improvvisati e non autorizzati che guidano le preghiere e che non offrono alcuna garanzia di non sfruttare tali momenti per far avvicinare i soggetti più deboli e privi di prospettive a forme di radicalismo politico-religioso.

Sempre con il provvedimento dell'ottobre 2001 la competenza territoriale per i delitti con finalità di terrorismo è stata centralizzata presso l'ufficio della Procura della Repubblica distrettuale – e parallelamente le funzioni di Gip sono state attribuite alla Sezione del capoluogo del distretto – al fine di non disperdere le conoscenze investigative in tanti rivoli a fronte di cellule che di norma si muovono e operano su un territorio più ramificato di quello di competenza di un singolo Tribunale.

to l'art. 270-*quater* che punisce chi arruola una o più persone per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo anche rivolta ad obiettivi "esteri" e l'art. 270-*quinquies* che punisce chi addestra o comunque fornisce istruzioni sulla preparazione o sull'uso di materiali esplosivi, di armi da fuoco o di altre armi, di sostanze chimiche o batteriologiche nonché di ogni altra tecnica per il compimento degli stessi atti di violenza di cui all'art. 270-*quater* e con la medesima finalità anche internazionale. Entrambe le nuove fattispecie costituiscono l'adeguamento interno alla Convenzione sulla prevenzione del terrorismo siglata a Varsavia il 16 maggio 2005[11] ma mentre nel caso di arruolamento è prevista la punibilità solo di chi arruola nel caso di addestramento è prevista la punibilità anche dell'addestrato[12].

[11] La Convenzione, adottata nell'ambito del Consiglio d'Europa è stata sottoscritta dall'Italia ed in vigore dall'1 giugno 2007. La Convenzione impegna gli Stati membri a punire come reati gravi l'apologia, il reclutamento e l'addestramento per il terrorismo, nel quadro comunque del rispetto dello stato di diritto, dei valori democratici, dei diritti umani e delle libertà fondamentali così come enunciate nella giurisprudenza della Corte Europea dei diritti dell'uomo.

[12] Con il provvedimento del 2005 è stato inoltre inserito nella legge 26 luglio 1975 n. 304 e cioè nell'Ordinamento penitenziario l'art. 18-*ter* che consente lo svolgimento dei colloqui a fini investigativi anche al fine «di acquisire dai detenuti o dagli internati informazioni utili per la prevenzione e repressione dei delitti commessi per finalità di terrorismo, anche internazionale, o di eversione dell'ordine democratico».

Si tratta di uno strumento che non gode sempre di buona stampa ma è invece utile, salva sempre l'inutilizzabilità processuale delle informazioni raccolte, ad acquisire spunti investigativi, ampliare il bagaglio di conoscenze della Polizia giudiziaria, è propedeutico a scelte di collaborazione del detenuto e in alcuni casi può contribuire a salvare vite umane. Si deve tuttavia ricordare che mentre nel terrorismo interno il colloquio tra l'appartenente alla Polizia giudiziaria e il detenuto si svolge quantomeno attraverso una "grammatica comune", nel caso di colloqui investigativi legati al terrorismo internazionale mancano alcune pre-condizioni che possono facilitare il contatto. Infatti la diversità delle basi culturali e dei codici di comunicazione tra gli operanti e l'interlocutore, la difficoltà di prospettare misure di protezione per i parenti che vivono all'estero e la profondità della ideologizzazione non solo in senso politico ma anche religioso del soggetto rendono più difficile il distacco dai valori inculcati all'interno della sua comunità e costituiscono un serio ostacolo all'esito positivo del colloquio. Sui colloqui investigativi così come ridefiniti dal legislatore del 2005 si veda G. SALVINI, *I colloqui*

Soprattutto nel provvedimento del 2005 il legislatore ha colto la necessità di definire anche direttamente all'interno del Codice penale in cosa consistano le condotte di terrorismo. A tal fine è stato inserito l'art. 270-*sexies* che trasporta quasi alla lettera nel codice la definizione fornita dalla Decisione Quadro del Consiglio dell'Unione europea del 13 giugno 2002[13].

L'art. 270-*sexies* e la Decisione Quadro hanno tra l'altro il pregio di fornire al giudice regole di interpretazione oggettiva e neutra rispetto a scelte di valore prescindono quindi da valutazioni, anche in senso larvato, politico-culturali in quanto definiscono il terrorismo non alla luce dei fini ultimi "giusti" o "ingiusti" ma piuttosto attraverso i mezzi usati e i beni umani e materiali colpiti.

Questo intervento si era reso necessario a fronte di provvedimenti giudiziari che avevano in sostanza giudicato espressione di legittima "guerriglia" l'invio di combattenti fondamentalisti dall'Italia, muniti di documenti falsi, in Iraq in prossimità dell'intervento delle forze della coalizione occidentale e con il compito di condurre in quel paese azioni

---

*investigativi e i permessi di soggiorno a fini investigativi per il contrasto del terrorismo*, in A.A. DALIA (a cura di), *op. cit.*, 1 e ss.

Inoltre l'articolo 4 del d.l. 27 luglio 2005 n. 144 ha esteso ai Servizi di informazione e per la sicurezza la possibilità di svolgere intercettazioni preventive quando «siano ritenute indispensabili per la prevenzione di attività terroristiche o di eversione dell'ordinamento costituzionale». Tali intercettazioni devono anch'esse essere autorizzate dal Procuratore Generale competente per territorio, non possono essere utilizzate nel procedimento penale e devono, esaurito il loro compito, essere distrutte.

Sulle intercettazioni preventive così come ampliate dal legislatore del 2005 si veda R. CANTONE, L.A. D'ANGELO, *Una nuova ipotesi di intercettazione preventiva*, in A.A. DALIA (a cura di), *op. cit.*, 45 e ss.

[13] L'art. 270-*sexies* indica quindi che sono considerate con finalità di terrorismo le condotte che: «possono arrecare grave danno ad un Paese o ad una organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i pubblici poteri o un'organizzazione internazionale a compiere o ad astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di una organizzazione internazionale…».

La Decisione Quadro 2002/475/GAI è pubblicata sulla Gazzetta Ufficiale n. 164 dell'Unione europea del 2 giugno 2002.

senza regole e senza quartiere tali da colpire deliberatamente in molti casi anche obiettivi civili e la stessa popolazione civile[14].

## *3. Arruolamento e* foreign fighters*: l'intervento legislativo del febbraio 2015*

Infine, ed è questa la fase attuale, poche settimane dopo la strage nella redazione del Charlie Hebdo, con il d.l. 18 febbraio 2015 n. 7[15] è

[14] La discussa sentenza con giudizio abbreviato emessa dal GUP presso il Tribunale di Milano il 24 gennaio 2005 nel procedimento a carico di Drissi Noureddine ed altri che esclude l'applicabilità dell'art. 270-*bis* c.p. nei confronti dei componenti delle cellule islamiche individuate a Milano è pubblicata in *Guida al Diritto*, 2005, fasc. 6, con un primo commento di Vincenzo Santoro e Giuseppe Frigo.

In senso del tutto difforme dal provvedimento del GUP di Milano dr.ssa Clementina Forleo si legga l'ordinanza di custodia cautelare emessa dall'Autore del presente intervento il 17 maggio 2005 in *Guida al Diritto*, 2005, fasc. 30, 78 e ss. con un commento di Vincenzo Santoro. Nel provvedimento si afferma che, anche prima del Decreto legge del luglio 2005, la Decisione Quadro del Consiglio d'Europa doveva costituire per il giudice un essenziale riferimento interpretativo e che era comunque improponibile considerare "guerriglia" o "insorgenza" e non terrorismo azioni che utilizzano in modo sistematico metodi terroristici: bombe nei mercati ed in genere tra la folla, sequestri ed uccisioni di ostaggi non solo occidentali, attacchi contro sedi dell'Onu e sedi diplomatiche, contro i luoghi di culto di minoranze religiose e così via. Per un commento nel senso indicato dall'ordinanza del 17 maggio 2005 si veda anche F. ROBERTI, *op. cit.*, 455, 488 e 504-506.

[15] Convertito con la legge 17 aprile 2015 n. 43. Per un commento si veda G. LEO, *Nuove norme in materia di terrorismo*, in *Diritto penale contemporaneo*, 2015; R. WENIN, *L'addestramento per finalità di terrorismo alla luce delle novità introdotte dal d.l. 7/2015*, in *Diritto penale contemporaneo*, 2015; S. COLAIOCCO, *Prime osservazioni sulle fattispecie antiterrorismo introdotte dal decreto legge n. 7 del 2015*, in *Arch. Pen.*, 2015, n. 1, 6 e ss. e il volume collettivo monografico R.E. KOSTORIS, F. VIGANÒ (a cura di), *Il nuovo 'pacchetto' antiterrorismo*, Torino, 2015.

Ci si limita in questa esposizione, per dare spazio soprattutto alle norme finalizzate ad affrontare i profili operativi del terrorismo internazionale, ad un semplice richiamo all'aggravante speciale dell'uso «dei mezzi informatici e telematici» introdotta dalla legge del 2015 per i reati di istigazione ed apologia di cui agli artt. 302 e 414 c.p. La medesima aggravante è prevista anche per il reato di addestramento a conferma della particolare attenzione dedicata dal legislatore all'utilizzo di tali mezzi che oggi costitui-

stato completato il dispiegamento dei mezzi di contrasto anticipando, sotto il profilo sostanziale, nei limiti dell'accettabile, la soglia di rilevanza penale e raffinando gli strumenti investigativi e preventivi.[16]

---

scono lo strumento principale per la diffusione del credo fondamentalista e il proselitismo.

Si segnala tuttavia in argomento la sentenza della Corte di Cassazione, Sez. I, 6 ottobre 2015 n. 47489 che ha confermato un'ordinanza di applicazione degli arresti domiciliari per il reato di apologia di cui all'art. 414 terzo comma c.p. aggravato, ai sensi dell'articolo 1 d.l. 625/79, dalla finalità di terrorismo nei confronti di un soggetto che aveva diffuso su Internet in italiano il documento intitolato *Lo Stato islamico: una realtà che ti vorrebbe comunicare* e cioè il manifesto "fondante" di propaganda dell'ISIS finalizzato al proselitismo.

[16] Infatti l'art. 6 del provvedimento ha introdotto la possibilità per i Servizi di informazione e sicurezza, su richiesta del Presidente del Consiglio dei Ministri anche a mezzo del Direttore Generale del D.I.S., di svolgere colloqui personali con detenuti e internati «al solo fine di acquisire informazioni per la prevenzione di delitti con finalità di terrorismo di matrice internazionale». I colloqui sono autorizzati dal Procuratore Generale competente per territorio e del loro svolgimento è data comunicazione allo stesso Procuratore Generale e al Procuratore Nazionale Antimafia e, ora, anche Antiterrorismo e al Comitato Parlamentare per la Sicurezza.

Si ponga attenzione al fatto che si tratta di colloqui non a fini investigativi come quelli condotti dalla Polizia Giudiziaria ai sensi dell'art. 18-*ter* Ordinamento penitenziario ma a fini preventivi attivati quando di norma non è ancora aperta o è solo all'inizio un'indagine penale ma l'attività di *intelligence* consente di cogliere situazioni sospette, segnali di pericolo, dati ancora frammentari di qualcosa in preparazione che deve essere anticipato e neutralizzato.

Si noti il parallelismo con quanto già previsto dal d.l. 18 ottobre 2001 n. 374 e dal d.l. 27 luglio 2005 n. 144 in materia di intercettazioni preventive effettuate dai Servizi centrali di Polizia giudiziaria e di colloqui investigativi e preventivi consentiti alla Polizia giudiziaria e ai Servizi di informazione (vedi note 9 e 11) come se i tre provvedimenti costituissero una "progressione" e quello del febbraio 2005 un completamento degli strumenti di contrasto imposto dal ripetersi e dall'aggravarsi, anche con tecniche nuove, delle azioni del terrorismo islamico

La duplice trasmissione comporta quindi un'osmosi tra controllo politico e controllo giurisdizionale. Un primo passo verso il venir meno dell'impermeabilità tra attività di *intelligence* e attività investigativa che dovrebbero sempre più convergere e coordinarsi, pur nella diversità del ruolo, quanto ad ambienti presi di mira e modalità strategiche per contrastare fenomeni criminali così raffinati, tecnicizzati e con alta capacità di movimento. Del resto delle attività di *intelligence*, relegata al passato la sua identificazione solamente con congiure e depistaggi, è assolutamente indispensabile nell'impegno contro il terrorismo internazionale. Si pensi ad esempio alle necessità di disporre di

Per soffermarsi soprattutto sugli aspetti sostanziali nell'art. 270-*quater* è stata introdotta la punibilità dell'arruolato, non prevista nel provvedimento del 2005, seppur con una sanzione più ridotta rispetto a quella prevista per l'arruolatore. L'art. 270-*quinquies*, nel confermare la punibilità anche del semplice addestrato, l'ha estesa anche alla persona che, avendo acquisito, anche autonomamente, istruzioni pone in essere comportamenti finalizzati alla commissione delle condotte di cui all'articolo 270-*sexies*[17].

Infine, quasi a completare questo microsistema di norme, l'art. 270-*quater*.1 ha introdotto la nuova fattispecie di organizzazione di trasferimenti per finalità di terrorismo che si applica a chi «organizza, finanzia o propaganda viaggi in territorio estero finalizzati alle condotte con finalità di terrorismo di cui all'art. 270 sexies».

Le nuove condotte punibili si modellano quindi esattamente sugli attori che nello scenario del terrorismo internazionale sono comparsi con prepotenza e provocato, con le azioni già avvenute e più ancora in prospettiva, i maggiori allarmi: i *foreign fighters*, stranieri residenti nei paesi europei e anche cittadini dall'origine o naturalizzati in tali Paesi, che partono per combattere a fianco dello Stato Islamico e i c.d. Lupi solitari che operano sganciati da gruppi e con semplice adesione ai loro proclami con un addestramento non più duale (con il rapporto addestra-

---

"antenne" all'estero e ai compiti posti dai sequestri di cittadini italiani in Medio Oriente e altri paesi. Spesso, di fronte a cellule molto mobili e che si formano intorno ad un unico progetto per poi colpire in un luogo in modo improvviso l'attività di *intelligence* è per sua natura anche più efficace, se ben condotta, di quella investigativa tradizionale nel parare i colpi e risparmiare vite umane. Essa infatti è rivolta al fine essenziale di prevenire gli attentati, non solo a quello di scoprirne gli autori, se ancora in vita, una volta avvenuti.

Sui colloqui preventivi nel provvedimento del febbraio 2015 si veda S. MARTELLI, *Colloqui a fini preventivi con detenuti e internati*, in R.E. KOSTORIS, F. VIGANÒ (a cura di), *op. cit.*, 45 e ss.

[17] Sulla necessità che, con una valutazione rigorosa, venga comunque accertato il requisito della concreta idoneità della condotta al perseguimento dei fini oggetto del duplice dolo specifico e cioè lo scopo di compiere atti di violenza o di sabotaggio a loro volta caratterizzati dalla finalità di terrorismo si veda A. VALSECCHI, *Le modifiche alle norme incriminatrici in materia di terrorismo*, in R.E. KOSTORIS, F. VIGANÒ (a cura di), *op. cit.*, 12.

tore – uno o più addestrati) ma da autodidatti, in genere grazie Internet e senza nemmeno essere in contatto diretto con i gruppi cui si ispirano.

È una metodologia terroristica, purtroppo in espansione, favorita dall'imprevedibilità tanto di coloro che sono intenzionati ad agire quanto dei possibili obiettivi. Una metodologia che ha colpito negli Usa e in Europa, in particolare in Francia, e la cui più recente espressione è stata la strage di Orlando negli Stati Uniti il 12 giugno 2016[18].

Un lupo solitario, quasi un precursore, è stato del resto Mohamed Game, l'autore dell'unico atto terroristico significativo di matrice islamica avvenuto in Italia, quello, già ricordato del 12 ottobre 2009 alla caserma dell'esercito Perrucchetti di Milano.

Proprio dal fenomeno dei lupi solitari emerge una profonda differenza tra il terrorismo interno, almeno quello di sinistra, legato al pensiero marxista e quindi al concetto di "Partito", e quello islamico derivante da una concezione religioso-millenarista.

Infatti nessuno avrebbe potuto compiere da solo un attentato a nome delle Brigate Rosse o di gruppi simili ed aspettarsi poi una legittimazione successiva da parte di tali organizzazioni. Ciò invece è possibile nello scenario mondiale del terrorismo islamico ed anzi ogni azione compiuta da un singolo che colpisca gli infedeli in luoghi ove non esista una cellula è raccomandata ed esaltata dall'ISIS come prima ancora lo è stata da Al Qaeda.

La principale obiezione che è stata mossa al gruppo di norme ora ricordato è la loro ridotta applicabilità in quanto ipotesi sussidiarie.

Infatti le condotte di arruolamento, addestramento e organizzazione di trasferimenti all'estero hanno un rilievo autonomo «fuori dai casi di cui all'art. 270 bis»[19] e cioè fuori dai casi di concorso nell'associazione con finalità di terrorismo. In tal modo lo spazio di intervento di queste norme sarebbe inesistente o molto residuale essendo possibile ed essen-

[18] Anche coloro che in Israele hanno aderito alla c.d. *intifada* dei coltelli aggredendo casuali passanti possono essere definiti lupi solitari in quanto di norma non hanno una precedente militanza in organizzazioni terroristiche e agiscono rispondendo a una "chiamata ideologica" rivolta indistintamente a tutti i musulmani che abitano in Israele.

[19] E l'art. 270-*quater* anche fuori dai casi di cui all'art. 270-*quater* cioè fuori dai casi in cui l'organizzatore o finanziatore del viaggio debba rispondere anche del più grave reato di arruolamento.

do la norma, in quasi tutti i casi simili procedere direttamente ad una contestazione di tipo associativo[20].

L'obiezione però, come quasi tutte le osservazioni "perfezionistiche" che provengono dalla dottrina, è eccessivamente critica.

Infatti da un lato le tre condotte ridefinite o introdotte dal legislatore completano razionalmente il sistema, anche in accordo con le Convenzioni internazionali. D'altro lato le difficoltà di provare la partecipazione ad una associazione internazionale, o meglio di definire i contorni e provare l'esistenza dell'organizzazione stessa[21], più sfuggente, fluida e priva di rigide gerarchie rispetto alle tradizionali organizzazioni terroristiche interne quali le BR e i gruppi affini, lasciano aperto un significativo spazio di applicazione di tali nuove fattispecie.

D'altronde l'elevato numero di *foreign fighters* partiti da numerosi paesi e le azioni sempre più frequenti dei Lupi solitari che si autoaddestrano e cercano di colpire al di fuori di un diretto inserimento in un'organizzazione, di cui in pratica conoscono solo le ideologie e i proclami, rendono utile disporre di tutti gli strumenti di contenimento e fanno ritenere più che prospettabili situazioni future in cui le nuove norme possano utilmente intervenire.

In sostanza la fattispecie di arruolamento in particolare risulterà applicabile quando il soggetto si sia "messo a disposizione", mettendosi in viaggio o cercando di mettersi in viaggio per l'estero ma non sia ancora entrato in concreto contatto con i componenti dell'associazione, salvo il propagandista che, in Italia o altrove, lo ha convinto ad arruolarsi.

## *4. Approcci giurisprudenziali e prime applicazioni*

Riallacciandosi un momento ai contrasti giurisprudenziali, già accennati, accesisi nel 2004-2005, e comunque prima dell'introduzione nel 2005 dell'art. 270-*sexies* c.p. che ha introdotto una accettabile definizione legale del concetto di terrorismo, sarebbe oggi del tutto supera-

[20] Si veda tra gli altri A. VALSECCHI, *op. cit.*, 6-8.

[21] Sulla difficoltà e complessità della prova del reato di cui all'art. 270-*bis* c.p., in particolare quando i gruppi esistenti in Italia svolgano compiti di mero supporto ad organizzazioni che operano in altri Paesi si veda F. ROBERTI, *op. cit.*, 486-488.

to parlare di una possibile antinomia combattenti-terroristi, estranei i primi sul piano associativo ad ogni possibile sanzione del Codice penale e sanzionabili solo i secondi.

Del resto, anche senza considerare le manifestazioni sempre più crudeli allestite in forma di "spettacolo" negli ultimi due anni dai gruppi cui i soggetti indottrinati e arruolati in Italia intendono unirsi, già nella fase precedente poteva apparire assai arduo dare una patente di legittimi resistenti, alle organizzazioni che nel 2002-2003 erano sostenute dall'Italia con l'invio di uomini, denaro e documenti. Basti ricordare ad esempio che Ansar al Islam, il gruppo al centro della sentenza "liberatoria" del GUP di Milano, non aveva alcuno scrupolo a colpire obiettivi civili e aveva inviato suoi giovanissimi *kamikaze* per colpire nel Kurdistan iracheno le persone presenti alla manifestazione annuale in ricordo della strage di El Halabia ove nel 1988 le forze di Saddam avevano ucciso col gas migliaia di civili. L'azione era stata sventata, gli attentatori suicidi bloccati ma se il piano avesse avuto buon esito si sarebbero aggiunte altre centinaia di vittime civili.

E oggi, in una nuova fase, si deve del resto ormai parlare, più ancora che di terroristi, di combattenti nemici in stato di guerra anche con il nostro Paese[22]. L'espressione può apparire troppo forte ma è lo stesso concetto di guerra, non più tra Stati riconosciuti ma tra tutte o quasi le entità statuali ed entità ideologico-militari di nuova formazione, ad essere cambiato. Lo stato di guerra non si dichiara più, come nei secoli passati, mandando un ambasciatore con una lettera di formale dichiarazione di apertura delle ostilità, formale dichiarazione la cui mancanza, come nel caso dell'attacco a Pearl Harbour, costituiva un illecito internazionale, ma origina quasi sempre da una situazione di fatto. E questa situazione di fatto si è pienamente realizzata con la formazione del c.d. Stato Islamico[23] in Siria e in Iraq. Uno Stato certamente non rico-

[22] Il conflitto in corso, se non si vuole utilizzare l'espressione "guerra", può definirsi a "bassa intensità" nei paesi occidentali mentre ha tutte le caratteristiche di un conflitto ad "alta intensità" in ampie zone del Medio Oriente.

[23] ISIS o più precisamente ISIL non è il nome di una organizzazione come Al Qaeda ma l'acronimo inglese di Islamic State in Iraq and the Levant mentre DAESH è l'acronimo, usato in modo in genere spregiativo, della medesima denominazione in lingua araba.

nosciuto dalla comunità internazionale ma che soddisfa i requisiti richiesti dal diritto internazionale: un governo, quello dell'ISIS con i suoi ministeri e le sue articolazioni amministrative, un popolo, anche se soggetto a un potere violento e un territorio di ampiezza non disprezzabile[24].

Uno scenario geopolitico quindi ben diverso da quello di Al Qaeda, un network internazionale che in pochi anni era stato in grado di disseminare le sue cellule, in grado di muoversi in modo autonomo, quasi in ogni parte del globo ma che disponeva solo di santuari e rifugi in zone remote del Pakistan e dell'Afghanistan e non ha mai controllato un territorio geograficamente riconoscibile.

Nei fatti e con i suoi proclami ufficiali lo Stato Islamico negli ultimi due anni ha dichiarato una guerra con intenti distruttivi, per quanto l'obiettivo possa essere velleitario, praticamente a tutto il resto del mondo: i paesi occidentali e in più ogni cittadino occidentale in quanto tale, i governi "apostati" del Medio Oriente, soprattutto quelli sciiti, tutti coloro che sono considerati altrimenti infedeli come la minoranza Yazida e in genere i fedeli delle religioni "non del Libro" oltre naturalmente ad Israele e a tutti gli ebrei in quanto tali. Sarebbe anche difficile applicare a tale situazione il termine di semplice "conflitto" che evoca

---

Il 29 giugno 2014 Abu Bakr Al Baghdadi aveva annunciato la nascita dell'ISIS nei territori compresi tra la Siria e Iraq sunnita, stato di cui si è autodichiarato Califfo. Da allora l'ISIS nei territori che controlla assolve tutti compiti di uno Stato: oltre ad avere proprie milizie che agiscono alla stregua di truppe regolari, dispone di un corpo di Polizia islamica per il rispetto dei precetti della Sharia, ha avviato un programma scolastico articolato su 12 classi, riscuote i tributi e paga i "dipendenti pubblici" e addirittura conia una propria moneta.

Lo Stato Islamico esiste quindi da poco più di due anni, un periodo breve ma non momentaneo sul piano dell'effettività, come Stato, del controllo di un territorio. Un periodo probabilmente percepito da molti come più lungo in ragione dell'orribile impatto e memoria mediatica delle sue azioni.

[24] Nel momento in cui rivediamo questo intervento e cioè nel dicembre 2016 lo Stato islamico sta perdendo considerevoli parti del territorio che controllava a seguito dell'offensiva in corso da due direzioni da parte delle forze curde e delle S.D.F. (Forze Siriane Democratiche) appoggiate dagli Stati Uniti e delle forze regolari irachene. Ma anche se nei prossimi mesi lo Stato Islamico andasse ad implodere i germi sparsi in numerose aree del globo resterebbero ancora in grado di colpire e si entrerebbe in una nuova fase del conflitto "asimmetrico" che ha segnato gli ultimi 15 anni.

qualcosa che si può comporre perché non si riesce ad immaginare quale trattativa possa essere avviata con l'ISIS.

In questa situazione di guerra dichiarata da una sola parte sarebbe stato pienamente possibile, invece di introdurre una norma penale specifica quale l'art. 270-*quater* c.p., applicare semplicemente, almeno nei confronti di chi è divenuto cittadino italiano, l'art. 242 del Codice penale che punisce, tra l'altro con l'ergastolo, «il cittadino che porta le armi contro lo Stato o presta servizio nelle forze armate di uno Stato in guerra contro lo Stato italiano»[25].

Può sembrare un punto di vista eccessivo ma, anche semplicemente utilizzandolo come ipotesi, serve a far comprendere quale sia stata l'evoluzione della minaccia costituita dal diffondersi del radicalismo islamico negli ultimi 15 anni.

Correttamente comunque il legislatore ha completato, con la riscrittura degli articoli 274-*quater* e 270-*quinquies* e l'introduzione dell'articolo 270-*quater.*1, il quadro degli strumenti a disposizione dell'autorità giudiziaria aggiornandolo all'evolversi – per non dire l'ulteriore degenerazione – di un fenomeno che ha reso più che mai interdipendente la situazione dei Paesi europei e quella del Medio Oriente.

In relazione al recente manifestarsi anche in Italia di arruolamenti in favore dell'ISIS e della conseguente organizzazione di viaggi in Siria sono interessanti alcuni provvedimenti di merito emessi a Milano, alcune ordinanze di custodia cautelare e una sentenza di primo grado, che hanno affrontato i profili attuali del fenomeno.

La vicenda descritta nella prima ordinanza di custodia cautelare emessa il 29 giugno 2015[26] rappresenta un caso da manuale del percor-

[25] O in alternativa, nei confronti sia del cittadino sia dello straniero, potrebbe essere applicato l'articolo 243 Codice penale che sanziona «le intelligenze con lo straniero affinché uno Stato estero muova guerra o compia atti di ostilità contro lo Stato italiano» o l'articolo 288 Codice penale che punisce «chiunque nel territorio dello Stato e senza approvazione del Governo arruoli o armi cittadini perché militino al servizio o a favore dello straniero».

[26] L'ordinanza nel procedimento 12285/14 GIP è stata emessa dal dr. Ambrogio Moccia nei confronti complessivamente di nove cittadini italiani e albanesi e di una cittadina dell'Arabia Saudita ed ha avuto vasta risonanza sia per la personalità di "Fatima" Sergio, la ragazza per prima convertitasi sia perché ha coinciso con il momento di maggior affluenza di *foreign fighters* dai paesi europei alla Siria.

so con il quale nel giro di breve tempo una famiglia italiana del tutto "normale" è transitata al radicalismo islamico e ha scelto di trasferirsi in Siria nel campo dell'ISIS.

Infatti al centro delle indagini vi è una famiglia di estrazione operaia residente nell'*hinterland* milanese da tempo convertitasi in blocco all'islamismo.

La più giovane delle due figlie si avvicina all'Islam nella sua versione più radicale, assume il nome di Fatima, sposa con un matrimonio islamico "combinato" in moschea un cittadino albanese anch'egli radicalizzatosi e insieme a questi, alla suocera e alla cognata che porta con sé un figlio piccolo raggiunge via Turchia i territori dell'ISIS.

In Siria Fatima si addestra all'uso delle armi e si rende disponibile a intraprendere il "martirio" per la causa della Jihad. Nel contempo si attiva per convincere i familiari rimasti in Italia a seguirla nella sua scelta, spiegando loro che l'*hjirah* cioè abbandonare le terre dei miscredenti per raggiungere quelle governate dai credenti è dovere di ogni buon musulmano. Esalta con i familiari le condizioni di vita nello Stato islamico dove ogni genere di conforto è assicurato in abbondanza dal "bottino di guerra". Racconta di aver assistito a decapitazioni e alla lapidazione di un giovane che aveva avuto un rapporto adultero con una donna destinata alla medesima sorte[27]. Ricorda ai familiari che l'uccisione degli occidentali miscredenti non è solo lecita ma doverosa.

Le lezioni impartite ai familiari dalla Siria coinvolgono tutti gli aspetti della loro vita privata e sociale in forma quasi di plagio: l'imminente divorzio della sorella maggiore deve essere considerato un dono di Allah perché in tal modo saranno rimossi tutti gli ostacoli terreni alla *hjirah* cioè alla partenza per le terre dell'Islam[28], il padre dovrà licenziarsi ottenendo la liquidazione e vendendo tutti i mobili di casa non

[27] Uccisione però, assicura Fatima, che avrà luogo, secondo la vera legge islamica, solo allo scadere dei due anni di vita del bambino prossimo a nascere in quanto fino a quel momento sarà consentito alla condannata allevarlo.

[28] Alla sorella maggiore Fatima assicura del resto la possibilità di contrarre un matrimonio a distanza con un combattente che diventerebbe poi il suo "tutore".

solo per disporre così dei soldi per il viaggio ma in modo da non lavorare più per i miscredenti[29].

Perfino i più elementari doveri familiari devono venir meno con il nuovo credo: la nonna anziana, che sarà lasciata in Italia, avrebbe bisogno di assistenza ma ella non è una convertita, è una miscredente e non vi è quindi alcun obbligo filiale nei suoi confronti[30].

Superata qualche titubanza, soprattutto da parte del padre, il gruppo dei familiari si appresta a partire per la Siria, progetto interrotto dall'esecuzione della misura cautelare.

Con il provvedimento del Gip a tutti gli indagati, in particolare a quelli che avevano già raggiunto la Siria, è stata contestata la partecipazione all'associazione con finalità di terrorismo internazionale, ma al padre e alla madre di Fatima, non ancora entrati nei ranghi dell'associazione, è stato invece contestato il nuovo reato di cui all'art. 270-*quater* primo comma c.p. e cioè l'organizzazione del viaggio finalizzato al raggiungimento con la figlia della Siria con le finalità di cui all'art. 270-*sexies* c.p.

Ciò sul presupposto, condivisibile, che l'organizzazione del trasferimento per finalità di terrorismo possa riguardare non solo soggetti terzi ma anche se stessi.

Si è trattato quindi, al di là delle responsabilità penali peraltro in parte già accertate[31], del primo provvedimento giudiziario di applica-

[29] Non è bene, secondo Fatima, lavorare per miscredenti perché la loro organizzazione del lavoro rende difficile la preghiera quotidiana e soprattutto perché sono gli occidentali che devono essere ridotti in schiavitù («sono loro che devono essere i nostri schiavi, non noi…», si sente infatti in una conversazione).

[30] Infatti «non c'è alcuna amicizia tra noi e i miscredenti», si sente in un'altra conversazione: «nessuna, neanche se sono padre e madre».

[31] La sorella maggiore di Fatima e tre altri imputati sono stati condannati con rito abbreviato in data 23 febbraio 2016 per il reato di partecipazione ad un'associazione terroristica internazionale a pene varianti tra i 5 anni e 4 mesi e 2 anni e 8 mesi di reclusione. Nella sentenza emessa dal GUP dr.ssa Donatella Banci Buonamici si legge che l'ISIS (a differenza di Al Qaeda, che non è mai riuscita ad organizzare un apparato statale radicato su un territorio) è «uno Stato terroristico» che nei territori controllati «ha stabilito precise competenze amministrative, giuridiche, tecniche, scientifiche e ha coniato una moneta» e dispone di un «sistema di riscossione dei tributi e di pagamenti di compensi dei combattenti e dei dipendenti pubblici», tutto ciò però appunto con fina-

zione della nuova fattispecie di reato in un caso tra l'altro, anche sul piano "culturale", estremamente istruttivo[32].

La rilevanza del reato di arruolamento e dell'art. 270-*quater* c.p. non si esaurisce comunque nella semplice e diretta applicazione della norma sostanziale punitiva.

Infatti lo stesso d.l. 18 febbraio 2015 n. 7, che ha ridefinito il reato, ha modificato anche la disciplina di cui al d.lgs. 159/11, il c.d. Codice Antimafia, in materia di misure di prevenzione personali. Ha disposto infatti con l'art. 4 che tali misure possano applicarsi anche ai soggetti che pongono in essere atti preparatori «a partecipare ad un conflitto in territorio estero a sostegno di una organizzazione che persegue le finalità terroristiche di cui all'art. 270 sexies c.p.». Si tratta quindi di soggetti che sono in procinto di essere arruolati per combattere a fianco di organizzazioni come l'ISIS e che sono ora passibili di misure di prevenzione come la sorveglianza speciale[33].

---

lità terroristiche di «eliminazione sistematica dei miscredenti e di espansione territoriale» che intende instaurare «un sistema di terrore contro chiunque, persone, Stati, intesi come Stati-comunità, organizzazioni internazionali». Gli imputati in stato di latitanza, giudicati con rito ordinario, sono stati condannati 18 dicembre 2016 dalla Corte di Assise a pene più severe, tra gli 8 e i 9 anni di reclusione. Tra di essi Fatima e la sua reclutatrice che operava dall'Arabia Saudita.

[32] Si aggiunga che le due sorelle erano state indottrinate non solo a livello locale tramite la frequentazione di una moschea lombarda ma grazie alle "lezioni" impartite via *skype* da una donna residente a Riyadh in Arabia Saudita. Le "lezioni" di dottrina esaltavano infatti le azioni dello Stato Islamico e propagandavano la necessità di unirsi all'ISIS in terra di Siria. La realtà dell'Arabia Saudita presenta del resto un doppio volto: paese politicamente stabile, "moderato" e filo-occidentale è nello stesso tempo uno dei principali motori di finanziamento, diffusione e di proselitismo all'estero in favore delle tendenze islamiche più radicali.

In Arabia Saudita tra l'altro è in corso, nel silenzio della comunità internazionale, una metodica campagna di persecuzione nei confronti degli "atei" in base ad una legge introdotta dal defunto re Abdullah che equipara gli atei ai terroristi in quanto il pensiero ateo minerebbe i fondamenti della religione islamica che è alla base dell'Arabia Saudita. Recentemente, tra i tanti casi, un *blogger* è stato condannato alla pena di 10 anni di carcere e a 2000 frustate per aver inviato un *tweet* di contenuto ateo rifiutando poi di pentirsi e insistendo che quello che aveva scritto rifletteva le sue convinzioni e che aveva il diritto di esprimerle.

[33] Nei confronti degli stessi soggetti, in attesa dell'udienza per l'applicazione della sorveglianza speciale o dell'obbligo di soggiorno, può essere disposta in via di urgenza

Una misura di prevenzione basata su questi presupposti è stata ad esempio adottata nel luglio 2016 dal Tribunale di Brescia[34] che ha applicato nei confronti di una giovane italiana convertita al radicalismo e che progettava di partire per la Siria la misura della sorveglianza speciale col divieto di lasciare il suo comune di residenza e anche di navigare in rete[35].

Una seconda misura di custodia cautelare in carcere è stata emessa poco tempo dopo, il 21 luglio 2015 dalla sezione GIP del Tribunale di Milano nei confronti di un cittadino tunisino e di un cittadino pakistano, quest'ultimo residente in provincia di Brescia[36].

In questo caso l'imputazione formulata è quella di quell'articolo 270-*bis* c.p. per aver partecipato all'organizzazione sovranazionale Stato Islamico definita terroristica, come si legge nell'ordinanza, anche dalla Risoluzione del 15 agosto 2014 del Consiglio di Sicurezza delle Nazioni Unite.

Le condotte contestate ai due indagati sono quelle di aver disseminato la piattaforma *twitter* di appelli inneggianti allo Stato Islamico[37] e soprattutto di essersi auto-addestrati, mediante manuali dell'ISIS reperibili in Internet, alla costruzione e al trasporto di ordigni, comprese autobombe[38] e, dopo aver arruolato un altro combattente, aver programmato la propria partenza della Siria per il mese di settembre.

I due avevano comunque in progetto, come emerge dalle intercettazioni anche informatiche, di compiere, prima di partire, un attentato al-

dal Questore la misura temporanea del ritiro del passaporto e degli altri documenti validi per l'espatrio, provvedimento che deve poi essere convalidato dall'Autorità giudiziaria.

[34] Tribunale di Brescia, Sezione Misure di Prevenzione, pres. Anna Di Martino.

[35] Il marito tunisino è stato invece espulso dall'Italia verso il suo paese di origine sulla base dell'art 13 comma 2 del d.lgs. 286/98 anch'esso integrato dal d.l. del 18 febbraio 2015 n. 7 che, a completamento del sistema, ha esteso la possibilità di espulsione allo straniero che abbia posto in essere con le stesse finalità atti preparatori per prendere parte ad un conflitto all'estero.

[36] Proc. n. 4449/15 GIP, giudice dr.ssa Elisabetta Meyer.

[37] Tra cui *tweet* che rappresentano la bandiera nera dell'ISIS issata su Roma.

[38] Altri manuali utilizzati degli indagati insegnano inoltre come mimetizzarsi («How to survive in the west») frequentando locali occidentali e bevendo o fingendo di bere alcolici in modo tale da non esser individuati come islamici radicali.

l'aeroporto militare e base Nato di Ghedi in provincia di Brescia e a tal fine avevano già effettuato alcuni sopralluoghi.

Non sono quindi stati contestati i reati di auto-addestramento e arruolamento[39] ma queste condotte costituiscono comunque l'elemento essenziale della condotta associativa contestata e qualora in taluni casi nelle fasi del giudizio di merito non dovesse essere ritenuta provata la concreta adesione all'organizzazione, i reati ridefiniti dal provvedimento del febbraio 2015 potrebbero essere presi in considerazione per sanzionare comunque le attività emerse nel corso delle indagini[40].

Una terza ordinanza di custodia cautelare, adottata sempre dalla sezione Gip del Tribunale di Milano[41], ha riguardato due gruppi familiari residenti in provincia di Lecco. Il primo nucleo all'inizio del 2015 si era trasferito in Siria per unirsi alle fila dell'ISIS mentre il secondo, al momento dell'arresto, era in procinto di partire[42].

---

[39] Uno dei due arrestati peraltro aveva già espresso il suo giuramento di fedeltà (denominato *bay'a*) al califfo Abu Bakr Al Baghadi.

[40] Nel caso ora esposto i due imputati sono stati condannati dalla Corte di Assise di Milano con sentenza del 25 maggio 2016 (pres. Ilio Mannucci Pacini, giudice estensore Ilaria Simi) alla pena di 6 anni di reclusione ciascuno per il reato associativo di cui all'art. 270-*bis* secondo comma c.p.

Nella motivazione della sentenza, che dà ampio spazio alle condotte di proselitismo, istigazione ed auto-addestramento non essendo ancora stati compiuti dagli imputati atti di terrorismo, si legge in modo semplice ma efficace che la concreta «esecuzione di un'azione terroristica segna anche il momento in cui l'intervento repressivo dello Stato è ormai inutile perché non vi sono più soggetti da punire (e da rieducare)» dato che i responsabili hanno già coronato la loro scelta politico-religiosa con il martirio. Proprio per questa ragione le scelte legislative europee e anche italiane hanno introdotto da un lato «nuovi strumenti di contrasto improntati ad una anticipazione dell'intervento repressivo» e d'altro lato la partecipazione all'associazione può essere configurata anche sulla base della semplice «messa a disposizione» della rete terroristica e anche in presenza di contatti ridotti o solo sporadici con componenti dell'associazione internazionale. Nel caso in esame infatti i due imputati stavano attuando il loro programma terroristico "guidati" solo da contatti via Facebook con esponenti dell'ISIS operanti a Raqqah in Siria e in Tunisia a Sousse ove il 26 giugno 2015 è avvenuta in spiaggia una strage di turisti.

[41] Proc. 996/16 GIP, ordinanza di custodia cautelare in data 26 aprile 2016, giudice dott.ssa Manuela Cannavale.

[42] La coppia già partita per la Siria, una donna italiana convertita e il marito marocchino, ha portato con sé tre bambini in tenera età. Un altro cittadino marocchino arresta-

Coloro che erano già giunti in Siria avevano ricevuto, come risulta dalle intercettazioni, addestramento militare ed avevano già partecipato ad azioni rendendosi disponibili anche al martirio. Inoltre coloro che erano arrivati per primi nel territorio dell'ISIS si erano adoperati affinché coloro che intendevano seguirli ricevessero personalmente la *takzia* e cioè la raccomandazione-autorizzazione ad arruolarsi inviata dalle autorità dello Stato Islamico.

Anche in questa indagine è stata elevata nei confronti di tutti gli indagati l'accusa di cui all'art. 270-*bis* c.p. ma anche in questo caso l'arruolamento e l'addestramento costituiscono l'aspetto centrale della vicenda processuale e valgono quindi le stesse considerazioni cui si è appena fatto cenno.

Di interesse, anche sul piano culturale, è l'invio ad uno degli indagati, accertato nel corso di questa indagine, da parte di un non identificato "Sceicco" di un testo denominato *Poema bomba* in cui tra l'altro si legge:

> Ascolta lo Sceicco, colpisci! dalle tue palme eruttano scintille e sgozza con il coltello, è attesa la gloria, fai esplodere la tua cintura nella folla dicendo "Allah Akbar"! esplodi come un vulcano, spaventa chi è infedele, affronta la folla del nemico ringhiando come un fulmine, pronuncia "Allah Akbar" ed esploditi o leone! …oh Stato islamico! accendi il fuoco sulla folla, versa sulla testa del crociato granate, non aver mai pietà finché non si spezza ogni vita tranne quella del popolo che ha combattuto da jihadista per Dio… guadagna il Paradiso come i primi combattenti e vai verso la gloria che chiama chi va verso essa. Grida Allah Akbar!

---

to quando era in procinto di partire è fratello di un *foreign fighter* caduto in Siria combattendo per le milizie dello Stato islamico. Nelle conversazioni del fratello con gli altri indagati si ascolta che il *foreign fighter* deceduto era riuscito, in soli tre mesi, a realizzare il "suo sogno" e cioè quello di morire da martire.

Questi era stato espulso dall'Italia all'inizio del 2015 con provvedimento del Ministro dell'Interno ed era inizialmente riparato in Svizzera. I provvedimenti di espulsione quindi, pur se molto utili nell'immediatezza, non proteggono da una "disseminazione" dei militanti in Europa né impediscono sempre la realizzazione del proposito di raggiungere le zone di conflitto.

Il testo non è solo un incitamento a commettere atti di violenza con finalità di terrorismo ma un esempio illuminante del condizionamento mentale attraverso le parole e la loro ossessiva ripetizione che caratterizza l'attività di indottrinamento e di proselitismo dell'Islam radicale.

Infine la sezione Gip di Milano ha emesso nel novembre 2016 un'altra ordinanza di custodia cautelare nei confronti di una cittadina albanese residente in provincia di Lecco che, dopo un indottrinamento via internet e un matrimonio *online* con un combattente già in Siria, ha raggiunto tale paese via Istanbul portando con sé il figlio più piccolo di sei anni[43]. L'indagata, tuttora in Siria, è latitante e quindi non è possibile disporre dell'ordinanza che tuttavia nello svilupparsi dei fatti e nell'approccio in diritto si colloca nella medesima linea dei provvedimenti già ricordati.

Si può quindi concludere che l'introduzione o la miglior definizione delle fattispecie di reato di cui agli artt. 270-*quater*, 270-*quater*.1 e 270-*quinquies* non rappresenta un semplice adeguamento a quanto previsto dalla Convenzione di Varsavia del 2005 e dalla Risoluzione 2178 del 24 settembre 2014 del Consiglio di Sicurezza delle Nazioni Unite[44] ma costituisce uno strumento processualmente utile e un segnale indispensabile sul piano preventivo e anche dal punto di vista culturale.

## *5. Qualche riflessione culturale*

La risposta non può tuttavia essere solo militare e nemmeno giudiziaria ma serve una corretta riflessione culturale che sia innanzitutto libera da atteggiamenti di autocensura e limitazione della sfera di giudizio razionale. È bene innanzitutto chiamare le cose con il loro nome, non alterare ciò di cui si parla se si vuole sconfiggerlo o almeno contenerlo.

[43] Gip dr.ssa Manuela Scudieri. Si veda *Il Corriere della Sera*, 16 dicembre 2016, ove si riferisce che il bambino, già avviato all'addestramento, sarebbe riuscito a comunicare per telefono un paio di volte con il padre in Italia dicendogli di voler tornare a casa per andare a scuola e, ove si trova, di avere paura perché «ci sono gli aerei che lanciano le bombe».

[44] Ove per la prima volta compare il concetto di "Combattenti terroristi stranieri".

Affermare che il terrorismo attivo in quasi tutti i continenti del mondo nulla abbia a che fare con l'Islam è un pensiero puerile[45].

Infatti il terrorismo di oggi nasce all'interno di un discorso religioso islamico. Tanto i radicali quanto i "moderati" sono entrambi figli dell'Islam. E purtroppo a molti sfugge il lato oscuro dell'impostazione che nega il rapporto Islam-terrorismo. Se i crimini dell'ISIS e di Al Qaeda nulla hanno a che fare con l'Islam perdono ogni significato gli sforzi nei confronti degli islamici "moderati" affinché reagiscano e trovino all'interno del mondo islamico anticorpi affinché eventi simili non si ripetano. Consente loro di stare in silenzio e, come troppo spesso è avvenuto, di stare alla finestra a guardare.

Negare che si tratti di terrorismo religioso è negare la comprensione delle sue origini. È sufficiente infatti nel coacervo contraddittorio del Corano[46] e anche tra gli *Hadith* del profeta, scegliere la *sura* e cioè il versetto che si preferisce, quella che esalta la violenza contro i miscredenti o quella più tollerante, perché ogni fedele possa collocarsi in una delle molte realtà dell'Islam, dalle più radicali alle più pacifiche, in una frammentazione resa tra l'altro possibile dalla mancanza di un'autorità religiosa centrale[47].

---

[45] Alcune Risoluzioni dell'Unione europea e le prese di posizione anche di alcuni autorevoli magistrati italiani che si occupano di questa materia raccomandano, ad avviso di chi scrive sbagliando decisamente, di non usare negli atti l'espressione *terrorismo islamico* bensì quella di terrorismo *tout court* o di terrorismo internazionale.

[46] Per un'esposizione accessibile della struttura e dei lineamenti essenziali del testo sacro dell'Islam si veda *Il Corano*, con prefazione e commento di Magdi Cristiano Allam e traduzione di Cherubino Mario Guzzetti, Milano, 2015

[47] Si ricordi che il Corano, parola non ispirata da Allah ma dettata direttamente da questi a Maometto, è stato composto in forma "diaristica" in quanto per tutta la vita il Profeta avrebbe ricevuto il verbo dall'unico Dio. Da ciò consegue che non tutte le sue parti sono tra loro congruenti come non sarebbe congruente un diario scritto per l'intera vita pur dalla medesima persona, il cui carattere e le cui inclinazioni variano nel tempo. In concreto la parte del Corano trasfusa da Maometto nella prima fase della sua vita presenta *sure* più tolleranti mentre nella seconda fase prevalgono le *sure* in cui si esalta l'eliminazione dei miscredenti. Da ciò consegue per ogni realtà mussulmana la possibilità di "scelta" in favore dell'una o dell'altra impostazione. Ovviamente tale analisi parte dal presupposto razionale, condiviso da chi scrive, che non si possa immaginare un Dio che "detta" un libro, opera invece dell'uomo.

Il seme di ogni deriva violenta esisteva del resto già dagli albori di questa fede, storicamente espansionistica e conflittuale.

L'Islam è infatti, non scordiamolo, l'unica grande religione fondata da un capo militare. L'Islam soprattutto tratta l'umanità "all'ingrosso". La sua espansione si è quasi sempre basata sulla conquista e non sulla convinzione. Conquistato un territorio, divenuto quindi *Dar al - Islam*, terra dell'Islam, i credenti o coloro che devono diventare tali sono semplicemente tutti coloro che vi abitano sopra[48]. Non c'è alcuna prospettiva, come nel Cristianesimo, di un Dio che parla alla coscienza del singolo uomo. Le scelte individuali del singolo, che del resto non ha alcun modo di rapportarsi con Allah ma deve solo obbedirgli, non hanno posto.

La sottomissione della coscienza individuale ha provocato nel tempo non pochi guasti. Basti pensare alla povertà della ricerca scientifica, con il suo portato di arretratezza, nei paesi islamici e basti confrontare la modesta normativa giuridica del Corano, fatta di imposizioni e di divieti anche bizzarri con il *corpus* del diritto romano, origine del diritto civile giunto sino a noi.

Ma tornando al problema dello scivolamento di tanti musulmani in tanti paesi verso il terrorismo dal quadro cultural-religioso ora accennato discende che il travaso è possibile in ogni momento e che si deve parlare di *transitabilità*.

Il cambiamento può essere immediato e questo aspetto non ha paragone con quello che vi è stato nel terrorismo interno.

Le Brigate Rosse e le organizzazioni similari impiegavano anni per "costruire" un militante regolare, un soggetto cioè, operaio o studente che fosse, disponibile a lasciare i relativi agi della vita normale e a passare alla clandestinità.

Nel terrorismo di matrice islamica non è affatto così.

La strage di Nizza, altri attentati avvenuti in Europa e altrove e il fenomeno dei *foreign fighters* offrono molti esempi di cambiamenti improvvisi che maturano nel giro di pochi giorni come un'infezione. Tan-

[48] Da qui la progressiva erosione in tutti paesi islamici delle comunità degli appartenenti ad altre fedi, il divieto o comunque le forti limitazioni a propagandare la propria fede e la proibizione assoluta dell'apostasia, spesso punita anche con la morte. Diventare musulmano non è una strada reversibile.

to l'immigrato senza storia quanto il musulmano di seconda generazione, tanto lo studente borghese come a Dacca quanto il piccolo malavitoso che sino a poco prima non frequentava nemmeno la moschea, possono transitare nel giro di poche settimane al radicalismo islamico e alla disponibilità a compiere azioni in suo nome.

La suggestione e la forza attrattiva operano spesso senza nemmeno il bisogno di un contatto diretto con esponenti del radicalismo, grazie alla mediazione di Internet e alla "chiamata" e agli appelli che vengono diffusi dai siti.

Questa caratteristica del nuovo terrorismo, insieme al numero infinito dei possibili obiettivi, aumenta esponenzialmente la pericolosità del fenomeno e vanifica spesso ogni strumento di prevenzione.

Vi è poi la questione del "multiculturalismo", parola entrata nel lessico comune ma senza comprenderne appieno il significato, fornirne un contenuto preciso.

È utile, per capire senza travisamenti, qualche esempio, tra i tanti possibili.

Suscita non poche preoccupazioni una recente sentenza della Corte costituzionale tedesca, ma in Inghilterra vi è stato anche di peggio[49], che ha dichiarato illegittimo il divieto di portare il velo per le insegnanti delle scuole pubbliche. Le conseguenze di questa sentenza rischiano di essere drammatiche per delle ragazzine di 10-12 anni, nel momento del loro primo affacciarsi sul mondo, che magari in casa conducono una battaglia quotidiana per non portare il velo e per altre libertà. Queste ragazzine verranno di sicuro iscritte nelle scuole con insegnanti velate e così anche la scuola contribuirà ad aumentare la pressione psicologica su queste ragazze.

Sempre più spesso in Francia, in Germania, in Inghilterra si evita, oltre alle vignette satiriche, di pubblicare libri, di rappresentare opere teatrali, di esporre opere d'arte perché offenderebbero la "sensibilità"

[49] L'Arcivescovo di Canterbury, capo della Chiesa anglicana, ha proposto l'istituzione di un sistema parallelo di *sharia* in Gran Bretagna con un aumento delle competenze del Consiglio Islamico per la *sharia* che in quel paese giudica già di matrimoni e divorzi musulmani. Fortunatamente la proposta è stata accolta con indignazione da buona parte dell'opinione pubblica.

dei credenti musulmani e provocherebbero l'ira e la reazione del mondo islamico.

Esempio simile di multiculturalismo trasformato in resa culturale è stata a Roma, in occasione della visita del presidente della Repubblica Islamica iraniana, la copertura delle statue che rappresentavano, anche in nudità, dei e personaggi dell'antichità.

Questo multiculturalismo è da rifiutare.

Lo Stato è formato da cittadini, non da tante comunità separate ciascuna con le sue leggi, comunità di cui qualcuna pretende di stabilire limiti alla libertà di tutti gli altri.

A questa visione, che tra l'altro anche all'interno di ogni comunità identitaria porta alla prevalenza dei più forti che pretendono di rappresentarla e alla sottomissione di tutti gli altri, non vanno contrapposti atteggiamenti di xenofobia o, peggio, indulgenze verso forme di razzismo.

L'unica strada rispettosa della Costituzione, delle nostre leggi e delle Convenzioni internazionali, prima di tutte quella sui Diritti dell'uomo, è quella del rafforzamento dell'*universalismo* dei diritti, da non confondere con il multiculturalismo, universalismo in ogni campo: nella famiglia, nelle espressioni sociali, quindi il diritto di studiare, lavorare, uscire, frequentare chi si vuole, nelle scelte religiose che devono appartenere solo alla coscienza dei singoli.

Lo Stato e la democrazia si costruiscono sulla cittadinanza, non tollerando ghetti monoculturali.

Che fare dunque?

Uno strumento per integrare senza cedere è rilanciare la Carta dei Valori promossa dal Ministro dell'Interno Giuliano Amato dopo un'ampia consultazione con i rappresentanti delle varie fedi e sottoscritta da questi ultimi nell'aprile 2007.

La Carta dei Valori e della Cittadinanza espone in modo semplice ed accessibile, più di quanto sia possibile nelle leggi ordinarie, i diritti e i doveri che riguardano gli immigrati e quindi specularmente quelli dello

Stato che li ospita[50]. Indica quindi il percorso per un'autentica integrazione ed eventualmente per l'acquisto della cittadinanza italiana[51].

La Carta dei Valori non è una legge, è un atto amministrativo ma un atto impegnativo e "fondante", una sorta di manuale esplicativo e "didattico" dei valori enunciati nella Costituzione che tocca tutti punti critici del rapporto tra gli immigrati e la nostra società. Si parla di diritto ad una retribuzione equa per lo straniero, del diritto-dovere dei figli degli immigrati di frequentare la scuola dell'obbligo, all'istruzione e diritto alla tutela della salute ma anche e soprattutto di libertà religiosa. E per libertà religiosa si intende non solo il diritto di professare la propria fede ma anche il diritto di non avere alcuna fede religiosa e il diritto di "apostasia" cioè di cambiare religione. Inoltre nella Carta sono esplicitamente condannate pratiche come la poligamia, i matrimoni forzati, ogni forma di coercizione all'interno della famiglia e le mutilazioni femminili. Ed è vietato aizzare in qualsiasi forma l'odio contro le altre religioni.

La Carta inoltre afferma che «la legge civile e penale è uguale per tutti a prescindere dalla religione di ciascuno ed unica la giurisdizione dei Tribunali per chi si trovi sul territorio italiano».

Esclude quindi fermamente per il futuro qualsiasi forma di sviluppo e di giurisdizione separata che trasformerebbe l'Italia non in un paese *multiculturale* ma in un paese, come si è detto, con tanti *monoculturalismi* in cui lo straniero avrebbe il diritto di assumere comportamenti contrari alle leggi con la giustificazione che essi sarebbero propri della comunità cui appartiene.

La Carta dei Valori dopo la sua approvazione è rimasta però confinata in una cerchia ristretta come se fosse stata sufficiente la sua sottoscrizione da parte dei capi delle comunità, in pratica gli unici o quasi a conoscerla, e fosse ad essi delegato il compito di diffonderla e di stimo-

[50] Ad esempio l'obbligo di corrispondere all'immigrato un compenso adeguato per il lavoro svolto e il rispetto nei loro confronti delle condizioni di sicurezza del lavoro, citati nella Carta, sono principi che devono trovare rispetto soprattutto da parte delle Autorità e dei datori di lavoro italiani.

[51] Diritto condizionato, si legge nella Carta, all'obbligo di conoscenza della lingua italiana.

lare da parte di tutti gli stranieri il rispetto dei principi e dei comportamenti che vi sono contenuti.

Una scelta disattenta, sbagliata, che ha ridotto la Carta quasi a lettera morta anche perché non è affatto escluso che alcuni dei capi delle comunità, soprattutto di quelle che di solito alzano di più la voce, l'abbiano sottoscritta solo con l'intento di ottenere una sorta di riconoscimento ma con la riserva mentale di osservarla e farla osservare il meno possibile[52].

Serviva invece e anche di più serve oggi che la Carta dei Valori possa raggiungere ogni singolo cittadino straniero.

È necessario quindi diffonderla nei momenti e negli ambiti sociali in cui lo straniero sta per venire a contatto o viene in contatto con i principi fondamentali delle leggi e della cultura italiana. Sarebbe quindi utile una sua diffusione nei Consolati italiani all'estero, in direzione, con una traduzione nella lingua del luogo, degli aspiranti immigrati e nei Centri di raccolta per profughi. È necessario anche illustrarla, senza timori di mancanza di rispetto verso le altre "culture", tramite i grandi mezzi di comunicazione e negli ambiti sociali quali scuola, sanità e associazioni sindacali in cui alcuni principi come quelli in materia di pluralismo religioso ed educativo, lavoro, diritto di famiglia e divieto di pratiche di mutilazione, sono suscettibili di diretta realizzazione.

E, per concludere, merita una riflessione la pretesa *islamofobia*, pseudoconcetto di cui si legge un giorno sì e un giorno no sulla stampa.

L'espressione *islamofobia* non è più di semplice uso giornalistico ma è presente sempre più spesso, in Francia e ora anche in Italia, in discorsi pubblici e anche negli atti giudiziari e nelle denunce di avvocati che sostengono stabilmente organizzazioni islamiche e denunciano pre-

[52] Vi è ad esempio fortemente da dubitare che il rifiuto di condannare l'apostasia sia condiviso con sincerità di intenti dai capi delle comunità islamiche che hanno sottoscritto la Carta. La condanna, o meglio l'impossibilità concettuale dell'apostasia, così come le severe sanzioni per la blasfemia, sono infatti principi essenziali della concezione islamica del mondo. Allontanarsi da Allah non può essere oggetto di alcuna scelta della coscienza individuale. Sia per l'uomo nato islamico sia per il convertito l'Islam è un'appartenenza irreversibile in quanto rappresenta la verità finale e la violazione di questa appartenenza non a caso è un crimine punibile con la morte in Arabia Saudita e in altri paesi islamici.

sunte discriminazioni o diffamazioni nei confronti di tale religione e dei suoi aderenti[53].

Ma *islamofobia* è solo un'invenzione che cerca di dare forma con un'espressione a qualcosa che non esiste nella realtà, quantomeno non esiste in quella italiana.

È una parola priva di contenuto che i *supporters* radicali dell'Islam sono riusciti accortamente a diffondere nel linguaggio comune e anche in quello istituzionale. Tecnicamente, per usare i termini degli studiosi del linguaggio, è un'"ipostasi", cioè l'artificio grazie al quale una parola non si riferisce ad una realtà che preesiste, per descriverla, ma la crea e dopo aver creato una realtà inventata consente di utilizzarla in molti modi tra cui colpire chi viene collocato all'interno di quella realtà fittizia. Infatti non vi è nessuna *islamofobia* in Italia. Nessuno è discriminato in quanto musulmano nei luoghi di lavoro, nelle scuole, negli asili, negli ospedali. Al più possono incontrare difficoltà in quanto stranieri ma non in quanto musulmani. Al contrario di molti paesi islamici, ove, per inciso, i lavoratori stranieri sono più che maltrattati, in cui il cristianesimo, l'ebraismo e l'intero Occidente vengono spesso ferocemente denigrati anche nei testi scolastici per i bambini.

Più semplicemente molti, sia cristiani sia laici, giudicano molto negativamente la religione islamica, e questa è una facoltà di giudizio e un diritto di critica garantiti a tutti dai tempi dell'Illuminismo. Si augurano che le violenze che alcuni seguaci del Corano tengono a mostrarci tutti i giorni via Internet e televisione non si propaghino al nostro paese e siano prevenute da chi ne ha il compito nell'ambito delle leggi, democratiche, che ci siamo dati. E questo è l'auspicio, legittimo, di tutti o quasi, certo non una "fobia" parola che tra l'altro evoca una malattia psichica.

E, per fare un esempio concreto che si riferisce ad uno dei dibattiti in corso in questo periodo, è indubbiamente sbagliato pensare di vietare il *burqini* e pensare di usare la polizia sulle spiagge per spogliare le bagnanti islamiche.

Ciò non toglie tuttavia che chiunque ha il diritto di scrivere e di sostenere in pubblico che paramenti simili sono frutto di una visione del

[53] L'*islamofobia* è molto inopportunamente menzionata anche in un atto per altri versi rilevante come la Carta dei Valori.

mondo arcaica e medioevale. E chiunque, soprattutto ha il diritto di esprimere che tutte le uniformi simili contengono germi di disprezzo e di razzismo perché comportano implicitamente l'idea radicata che tutti gli altri, bagnanti e non, siano esseri umani pericolosi dai quali è meglio nascondersi.

Dire questo non è *islamofobia* ma semplice esercizio del diritto alla libertà di pensiero e del diritto di critica cui l'islamismo, come qualsiasi altra credenza, non può avere il privilegio di sottrarsi.

In pratica l'*islamofobia* è un pretesto che serve solo a giustificare il proprio risentimento, le convulsioni del proprio mondo e spesso il fallimento del proprio sistema culturale

Il filosofo del linguaggio Ludwig Wittgenstein scriveva che la più grande violenza che si può fare è quella attraverso le parole, snaturandole e creando con esse incantesimi. E una di queste parole usata per fare violenza alle cose è appunto *islamofobia*. Non bisogna cadere in questo tranello.

*L'«uomo di vetro» è, storicamente, metafora totalitaria perché, reso un omaggio di facciata alle virtù civiche, nella realtà lascia il cittadino inerme di fronte a chiunque voglia impadronirsi di qualsiasi informazione che lo riguardi.*
(Stefano Rodotà)

*Nessuna 'anima bella' può sottovalutare la gravità del* terrorismo *internazionale.*
(Giorgio Marinucci)

# UNA RIFLESSIONE COMPARATA SULLE NORME IN MATERIA DI ADDESTRAMENTO PER FINALITÀ DI TERRORISMO[*]

*Roberto Wenin*

SOMMARIO: *1. Introduzione. 2. Normativa sovranazionale di riferimento. 3. La previsione normativa italiana in materia di addestramento per finalità di terrorismo. 4. La condotta del fornire istruzioni e dell'addestramento. 5. La finalità di terrorismo come strumento atto a delimitare la fattispecie. 6. Una norma, più fattispecie? 6.1. La soluzione adottata dagli ordinamenti stranieri. 6.2.1. La consapevolezza dell'addestratore circa la finalità terroristica in capo all'allievo. 6.2.2. La punizione della condotta del fornire istruzioni. 7. L'acquisizione di istruzioni per finalità terroristiche. 7.1. La nozione dell'acquisire. 7.2. Comportamenti univocamente finalizzati alla commissione di condotte terroristiche. 8. Alcune riflessioni di sintesi. 8.1. Il ricorso alle aggravanti dell'utilizzo del mezzo informatico e telematico. 8.2. La "trasformazione" del diritto penale classico. 8.2.1. Quale ruolo per la magistratura? 8.3. Vegliate, dunque.*

[*] La pubblicazione del presente contributo è stata anticipata, salve alcune limitate modifiche, sulla *Rivista trimestrale diritto penale contemporaneo*, 4, 2016, 108 ss.

## *1. Introduzione*

Il terrorismo rappresenta una fra le sfide più pressanti con le quali è chiamata a confrontarsi la moderna società. Non si tratta di un fenomeno in sé né nuovo, né tantomeno ignoto, tuttavia, esso pare aver acquisito connotati e peculiarità che lo portano a distinguersi da realtà criminali passate. Il terrorismo internazionale di matrice islamica si differenzia sia dal terrorismo interno[1], sia dalle organizzazioni criminali nazionali[2] per le finalità perseguite, le modalità esecutive del suo piano criminoso e in particolare per i mezzi di cui esso si serve. Rispetto al passato rimane per certi versi invariata, se non addirittura intensificata, la finalità intimidatoria. Il termine terrorismo deriva, come noto, dal latino *terrere* (atterrire)[3]. Quanto alla sua origine storica il termine fu utilizzato durante la rivoluzione francese per descrivere la crudeltà e carica intimidatoria dei metodi di governo utilizzati nel periodo che va dal 31 mag-

[1] Per usare una frase fatta, come dice M. LOMBARDI, *Il terrorismo nel nuovo millennio*, Milano, 2016, 1, «neppure il terrorismo è più quello di una volta»; «il terrorismo del nuovo millennio è altro e, forse, non è neanche più terrorismo, se lo leghiamo alle conoscenze consolidate».

[2] Cfr. R. BARTOLI, *Lotta al terrorismo internazionale. Tra diritto penale del nemico* jus in bello *del criminale e annientamento del nemico assoluto*, Torino, 2008, 203 ss.; ID., *Le nuove emergenze terroristiche: il difficile rapporto tra esigenze di tutela e garanzie individuali*, in questo volume; F. ROBERTI, *Le nuove fattispecie di delitto in materia di terrorismo*, in A.A. DALIA (a cura di), *Le nuove norme di contrasto al terrorismo. Commento al Decreto-legge 27 luglio 2005, n. 144 convertito, con modificazioni, nella Legge 31 luglio 2005, n. 155 ed integrato dal Decreto-legge 30 dicembre 2005, n. 272, convertito, con modificazioni, nella Legge 21 febbraio 2006, n. 49 e sintesi dei lavori parlamentari*, Milano, 2006, 449 ss.; A. PICCI, voce *Terrorismo (profili criminologici e giuridici)*, in *Dig. disc. pen.*, *Aggiornamento*, Torino, 2010, 822 ss., il quale ritiene preferibile il termine «radicalismo» che meglio individuerebbe quell'universo in cui possono essere riscontrate differenti correnti di pensiero e di azione; L. STAFFLER, *Politica criminale e contrasto al terrorismo internazionale alla luce del d.l. antiterrorismo del 2015*, in *Arch. pen. web.*, 2016, n. 3, 7 ss. Sul fenomeno del jihadismo in Italia si veda: L. VIDINO, *Il jihadismo autoctono in Italia: nascita, sviluppo e dinamiche di radicalizzazione*, Milano, 2014. Cfr. anche F. FASANI, *Terrorismo islamico e diritto penale*, Padova, 2016.

[3] Più precisamente il termine terrore deriverebbe dal latino *terror - oris*, a sua volta derivato di *terrēre*.

gio 1793 (espulsione dalla Convenzione dei Girondini) al 9 termidoro, cioè al 27 luglio 1794 (caduta di Robespierre). L'intimidazione rappresenta, dunque, un elemento caratteristico del metodo terroristico[4], che mira soprattutto ad avere un impatto attraverso la comunicazione, con la naturale conseguenza che la rete globale, per le sue caratteristiche massmediatiche, rappresenta lo strumento principe per la diffusione del "messaggio di terrore"[5]. Non solo la rete rappresenta un mezzo d'attuazione della finalità intimidatoria, ma costituisce al contempo uno strumentario atto a realizzare il piano criminoso tramite condotte di proseli-

[4] Tale elemento qualificante il terrorismo viene recepito nelle definizioni normative; così l'art. 270-*sexies* c.p. – che di fatto ricalca pressoché pedissequamente l'art. 1 della decisione quadro 2002/475/GAI del 13 giugno 2002 sulla lotta contro il terrorismo – stabilisce che: «Sono considerate con finalità di terrorismo le condotte che, per la loro natura o contesto, possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia».

[5] Cfr. UNODC, *The use of the Internet for terrorist purposes*, New York, 2012, reperibile sul sito: *www.unodc.org*; U. SIEBER, P.V. BRUNST, *Cyberterrorism - The use of the Internet for terrorist purposes*, Strasbourg, 2007. Si è precisato, G. CESTA, *Al Qaeda e i Media: strategie di comunicazione*, in *Gnosis Rivista italiana di intelligence*, 2011, n. 4, facendo riferimento alla strategia mediatica adottata dopo l'11 settembre 2001, che «La nascita delle cosiddette "guerre asimmetriche" nell'ultimo decennio, dove eserciti regolari fronteggiano un nemico non perfettamente identificabile da un'altra divisa, ha portato alla consapevolezza che, oramai, le guerre si combattono su fronti diversi – come quello mediatico – molto più che in passato. La guerra psicologica è sempre stata una delle armi nella faretra dei generali, fin da tempi molto lontani. Tuttavia, era un'arma che aveva una portata limitata e il suo impiego era visto come collaterale alle operazioni belliche "tipiche". Invece, da quando è stata dichiarata guerra aperta al terrorismo internazionale, il lato psicologico del conflitto a tratti è divenuto predominante, sospinto ed esasperato da quella fazione che aveva uno svantaggio militare in senso stretto e che, per questo, ha puntato su una strategia "innovativa". L'utilizzo dei Media da parte della galassia jihadista è esattamente il paradigma di questa nuova guerra mediatica che si combatte più nelle menti e nel cyberspazio che sul terreno, sul campo di battaglia».

tismo, di addestramento, reclutamento, e attività logistiche finalizzate alla preparazione di attentati per fini terroristici[6]:

> Internet è utilizzato per ispirare e mobilitare reti terroristiche locali e singoli individui in Europa e costituisce inoltre una fonte di informazioni sulle risorse e sui metodi terroristici, fungendo così da «campo di addestramento virtuale». Attività quali la pubblica provocazione per commettere reati di terrorismo, il reclutamento e l'addestramento a fini terroristici si sono moltiplicate ad un costo e con un rischio estremamente bassi[7].

In tale contesto occorre chiedersi quale ruolo possa spettare al diritto penale, il quale si trova sempre più esposto a scenari complessi i cui elementi caratterizzanti, legati allo sviluppo tecnologico, sono dati dalla dimensione globale, dalla delocalizzazione, dalla disomogeneità di valori:

> il sogno di una crescita del benessere necessariamente continua si è infranto, la mobilità reale e virtuale si è esasperata in frenesia motoria, la solida pianta delle nostre radici si è capovolta interrando la chioma[8].

Si tratta di un nuovo tipo di conflitto[9] che si serve talora di un luogo virtuale, delocalizzato e, al contempo, globalizzato, e obbliga a riconsi-

---

[6] Cfr. L. STAFFLER, *op. cit.* in nota 2, 16 ss. Sul ruolo in particolare dei *social network* si veda A. TENTI, *Isis e social network. Da Twitter a Facebook passando per WhatsApp e YouTube*, in *Gnosis Rivista italiana di intelligence*, 2015, n. 4, 75 ss.

[7] Dal preambolo della Decisione quadro 2008/919/GAI del consiglio del 28 novembre 2008 che modifica la decisione quadro 2002/475/GAI sulla lotta contro il terrorismo.

[8] M. LOMBARDI, *op. cit.* in nota 1, 7.

[9] M. LOMBARDI, *op. cit.* in nota 1, 11 ss. In realtà l'autore usa il termine guerra, termine rispetto al quale, tuttavia, per varie ragioni, si impone particolare cautela nell'uso, soprattutto quando si passa a riflettere sugli strumenti reattivi: cfr. L. FERRAJOLI, *Due ordini di politiche e di garanzie in tema di lotta al terrorismo*, in *Terrorismo internazionale. Politiche della sicurezza. Diritti fondamentali*, *Edizione speciale QG*, settembre 2016, 9: «si tratta di una nuova forma di guerra, generata dalla medesima logica della globalizzazione che abbiamo competentemente incorporato nella densa rete di relazioni con la quale interpretiamo il sistema della comunicazione, quello dell'economia e quello della politica, ma che non abbiamo ancora accettato per i medesimi effetti

derare i problemi di disciplina, anche futura, in una prospettiva essenzialmente sovranazionale.

Le tensioni cui è esposta la moderna società e di riflesso il diritto penale impongono forse di rimeditare le categorie tradizionali, nonché le stesse funzioni e i limiti del diritto penale[10]. Tale acquisita consapevolezza permette al contempo di evitare una sovraesposizione del diritto penale o una sua torsione, tenendo ferma l'essenza dei suoi principi di derivazione liberale. La rete informatica globale, nella sua dimensione virtuale, rappresenta spesso un mondo parallelo a quello reale, nel quale si infrangono i tradizionali limiti dimensionali, come ad oggi conosciuti. Si tratta di una realtà acefala, al contempo luogo primario di manifestazione delle libertà, nonché dello sviluppo economico e sociale, e occasione di proliferazione di attività criminali.

Se da un lato John Perry Barlow proclama l'indipendenza del cyberspazio:

> governi del Mondo, stanchi giganti di carne e di acciaio, io vengo dal Cyberspazio, la nuova dimora della Mente. A nome del futuro, chiedo a voi, esseri del passato, di lasciarci soli. Non siete graditi fra di noi. Non avete alcuna sovranità sui luoghi dove ci incontriamo[11]

dall'altro la giustizia invoca la sovranità del diritto:

---

che ha nella rimodellizzazione dei conflitti. Oggi la guerra non è più confinata su un territorio geografico, ma si estende con micro azioni connesse che la esportano ovunque…».

[10] Si è correttamente precisato che «la consapevolezza dei limiti del diritto può forse essere fonte di frustrazione, ma induce ad una maggiore sobrietà nell'affrontare le questioni difficili, evitando di immaginare che vi siano soluzioni magiche, e che il diritto penale sia la bacchetta del mago»: A. BEVERE, V. ZENO-ZENCOVICH, *La rete e il diritto sanzionatorio. Una visione d'insieme*, in *Dir. inform.*, 2011, 380.

[11] Dichiarazione pubblicata *online* nel febbraio del 1996 in risposta all'emanazione del *Telecommunications Act* del 1996 sotto il governo Clinton: «Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather». Testo completo disponibile sul sito: *www.eff.org/cyberspace-independence*.

> Non esiste nemmeno la sconfinata prateria di internet dove tutto è permesso e niente può essere vietato, pena la scomunica mondiale del popolo del web. Esistono, invece, leggi che codificano comportamenti e che creano degli obblighi, obblighi che, ove non rispettati, conducono al riconoscimento di una penale responsabilità[12].

Tra gli estremi di tali affermazioni di principio, occorre, in un'ottica di sano realismo, interrogarsi su quale possa essere il concreto ed effettivo ambito di operatività del diritto, consapevoli del fatto che un diritto penale senza una reale possibilità di coercizione, non solo sarebbe inutile, ma finirebbe per minare la sua stessa credibilità. Il diritto penale è stato, infatti, come noto, paragonato ad una spada il cui filo si deteriora per l'uso eccessivo[13]. Ciò cui si intende fare riferimento in questa sede non è, evidentemente, al diverso e noto dibattito circa l'opportunità, in particolare nell'ambito delle misure preventive, di ricorrere a strumenti diversi ed alternativi al diritto penale al fine di evitare contaminazioni con meccanismi di pura neutralizzazione[14], bensì i riflessi legati ad

[12] Tribunale di Milano, sentenza 24.02.2010 n. 1972, a firma del dott. Oscar Magi, 95; reperibile sul sito *www.penalecontemporaneo.it*. Sentenza pronunciata nel noto caso Google/Vivi Down nella quale ci si interrogava sugli obblighi gravanti in capo agli ISP.

[13] Cfr. C. PRITTWITZ, *Das deutsche Strafrecht: Fragmentarisch? Subsidiär? Ultima ratio? Gedanken zu Grund und Grenzen gängiger Strafrechtsbeschränkungspostulate*, in INSTITUT FÜR KRIMINALWISSENSCHAFTEN FRANFKURT AM MAIN (a cura di), *Vom unmöglichen Zustand des Strafrechts*, Frankfurt am Main, 1995, 402 ss. Per i rischi legati all'ineffettività dello strumento penale, in particolare nell'ottica pan-penalista e dell'ipertrofia penale che caratterizza in particolare l'esperienza italica, sia consentito rinviare, anche per i necessari riferimenti bibliografici, a R. WENIN, *Disposizioni sull'addestramento nell'uso di armi: un sintomo della degenerazione della coerenza sistemica?*, in *Riv. it. dir. proc. pen.*, 2014, 1893 ss.

[14] Sul punto si veda F. VIGANÒ, *Terrorismo, guerra e sistema penale*, in *Riv. it. dir. proc. pen.*, 2006, 648 ss., ad avviso del quale «il diritto e la giurisdizione penale sono il migliore *antidoto* contro i rischi di scivolamento verso derive intollerabili per lo Stato liberale di diritto e per la nostra stessa identità culturale occidentale, o giudaico-cristiana, della quale tanto oggi si discute» (680) e che «Minimizzare il rischio di errori ed abusi nella lotta al terrorismo – dalla reclusione di un innocente alle torture di un prigioniero – costituisce insomma un imperativo pratico dettato dal buon senso, prima ancora che dai principi fondanti della nostra civiltà giuridica, o da una qualsiasi immagine astratta dello "stato di diritto". E il diritto e la giurisdizione penale, ribadisco, costituiscono il migliore antidoto disponibile contro il rischio di simili errori ed abusi»

un'inevitabile ineffettività dovuta all'inidoneità dello strumento rispetto allo scopo perseguito[15].

La prima difficoltà risiede, come visto, nell'individuazione delle caratteristiche e peculiarità del fenomeno criminoso che si desidera contrastare. In senso critico si è, infatti, osservato come le modifiche normative nascano spesso da un pregiudizio in ordine al "nemico" che si vorrebbe "combattere"[16], ma non riescano infine a descriverne adeguatamente i connotati[17].

La difficoltà nel definire adeguatamente da un punto di vista normativo il fenomeno terroristico[18] si cumula poi alla "fretta" che spesso ac-

(684). Circa l'attualità del pensiero si segnala come il contributo citato sia stato di recente richiamato dallo stesso autore nel commentare le modifiche introdotte con il d.l. 18 febbraio 2015, n. 7: F. VIGANÒ, *Minaccia dei 'lupi solitari' e risposta dell'ordinamento: alla ricerca di un delicato equilibrio tra diritto penale, misure di prevenzione e tutela dei diritti fondamentali della persona*, in R.E. KOSTORIS, F. VIGANÒ (a cura di), *Il nuovo 'pacchetto' antiterrorismo*, Torino, 2015, XII s.

[15] Sul punto sia permesso rinviare al già citato scritto: R. WENIN, *Disposizioni sull'addestramento…*, cit. in nota 13, 1893 ss.

[16] La scelta della terminologia adottata è per molti versi significativa. Si è parlato di "lotta al terrorismo", "guerra al terrorismo", "contrasto al terrorismo". Al di là dell'apparente vicinanza semantica, la diversa scelta terminologica porta, talora, ad emersione, al di là delle finalità comunicative della politica, una diversità nell'approccio, non solo metodologico, ma altresì "valoriale". Guardando a recenti dibattiti, è noto lo scalpore sorto nella comunità scientifica intorno alla definizione di un diritto penale del nemico, intesa dal suo autore come mera descrizione di una realtà fenomenica, ma che rischia di offrire un fondamento teoretico ad una scelta valoriale.

[17] A. MARTINI, *La nuova definizione di terrorismo: il D.L. n. 144 del 2005 come convertito con modificazioni in L. 31 luglio 2005*, *n. 155*, in *Studium Juris*, 2006, 1230.

[18] Sulla definizione di terrorismo nell'ambito dell'esperienza italiana, che dovrebbe ricavarsi come noto dall'art. 270-*sexies* c.p., si veda, senza alcuna pretesa di esaustività: L.D. CERQUA, *La nozione di «condotte con finalità di terrorismo» secondo le fonti internazionali e la normativa interna*, in C. DE MAGLIE, S. SEMINARA (a cura di), *Terrorismo internazionale e diritto penale*, Padova, 2007, 55 ss.; A. MARTINI, *op. cit.* in nota 17, 1217 ss.; V. MASARONE, *Le* «condotte con finalità di terrorismo» *(art. 270*-sexies *c.p.): un'emergenza indeterminata*, in S. MOCCIA (a cura di), *I diritti fondamentali della persona alla prova dell'emergenza*, Napoli, 2009, 137 ss.; M. PELISSERO, *Delitti di terrorismo*, in ID. (a cura di), *Reati contro la personalità dello Stato e contro l'ordine pubblico*, Torino, 2010, 159 ss.; L. PISTORELLI, *Punito anche il solo arruolamento*, in *Guida dir.*, 2005, n. 33, 58 ss.; S. REITANO, *Riflessioni in margine alle nuove fattispecie*

compagna gli interventi del legislatore in prossimità di gravi attentati, nello sforzo di mandare un messaggio di sicurezza alla popolazione, emotivamente scossa[19]. Se, tuttavia, scopo precipuo dell'intervento

*antiterrorismo*, in *Riv. it. dir. proc. pen.*, 254 ss.; F. ROBERTI, *op. cit.* in nota 2, 445 ss.; G. SALVINI, *L'associazione finalizzata al terrorismo internazionale: problemi di definizione e prova della finalità terroristica*, in *Cass. pen.*, 2006, 3366 ss.; A. VALSECCHI, *I requisiti oggettivi della condotta terroristica ai sensi dell'art. 270* sexies *c.p. (prendendo spunto da un'azione dimostrativa dell'*Animal Liberation Front*). Nota a Tribunale di Firenze (Uff. GIP), ord. 9 gennaio 2013, Giud. Pezzuti*, in *Dir. pen. cont.*, 21 febbraio 2013; ID., *La definizione di terrorismo quale esempio dell'efficacia e della vincolatività delle fonti internazionali nell'ordinamento italiano*, in C. RUGA RIVA (a cura di), *Ordinamento penale e fonti non statali. L'impatto dei vincoli internazionali, degli obblighi comunitari e delle leggi regionali sul legislatore e sul giudice penale. Atti delle sessioni di studio tenutesi a Milano il 21 novembre 2005, il 10 marzo e il 24 marzo 2006*, Milano, 2007, 99 ss.; ID., *La definizione di terrorismo dopo l'introduzione del nuovo art. 270*-sexies *c.p.*, in *Riv. it. dir. proc. pen.*, 2006, 1103 ss.; ID., *Brevi osservazioni di diritto penale sostanziale*, in *Dir. pen. e proc.*, 2005, 1222 ss.; F. VIGANÒ, *La nozione di 'terrorismo' ai sensi del diritto penale*, in F. SALERNO (a cura di), *Sanzioni «individuali» del Consiglio di Sicurezza e garanzie processuali fondamentali. Atti del convegno di studio organizzato dall'Università di Ferrara (12 e 13 dicembre 2008)*, Padova, 2010, 193 ss.; si veda anche la sentenza Cass. pen., sez. VI, 15 maggio 2014 (dep. 27 giugno 2014), n. 28009, in *Dir. pen. cont.*, 30 giugno 2014, con nota di S. ZIRULIA, *No Tav: la Cassazione fissa i parametri interpretativi in merito alle condotte di attentato ed alla finalità di terrorismo.*

[19] Così nell'evidenziare l'opportunità di procedere a celere conversione in legge del decreto Pisanu, d.l. n. 144, del 27 luglio 2005 («Misure urgenti per il contrasto del terrorismo internazionale»), emanato dopo gli attentati di Londra, si precisò che «i cittadini devono sapere che lo Stato e le istituzioni sono in grado di affrontare i pericoli e le minacce del terrorismo internazionale, devono recepire la presenza degli organi preposti alla loro sicurezza come efficiente e sicura. In una concezione di questo tipo siamo certi che l'irrigidimento di alcune norme di pubblica sicurezza, l'introduzione nell'ordinamento di nuove fattispecie di reato, corrispondenti alle nuove, terribili, modalità di azioni dei terroristi verranno accolte dalla popolazione come giuste e necessarie» (N.F. FILIPPELLI (Misto-Pop-Udeur), *Resoconto stenografico della 857ª seduta del Senato di data 28 luglio 2005*, 72), aggiungendo poi che «un altro elemento che non si deve sottovalutare è rappresentato dall'effetto annuncio, volto a dare all'esterno un'immagine che tranquillizzi i cittadini che si sentono smarriti» (C. MARINI (Misto-SDI-US), *Resoconto stenografico della 857ª seduta del Senato di data 28 luglio 2005*, 59). Nell'ambito del dibattito parlamentare in sede di conversione del d.l. 7/2015 in senso critico si evidenziava che «D'altronde, la paura del terrorismo è anch'essa una manna dal cielo per chi ci governa, perché dispone i popoli, anche il nostro purtroppo, a rinun-

normativo è quello di portare un messaggio rassicurante alla popolazione[20], il rischio che si corre è allora quello di una normativa infine sfuocata rispetto al fenomeno che si "mira" a contrastare, in quanto ci «si preoccupa degli effetti sulla società e non della funzionalità ed efficienza della soluzione in termini politico-criminali»[21].

La riflessione che precede rischia, tuttavia, di sovrapporre distinti profili di analisi che pare opportuno esplicitare e tener distinti.

Da un lato si pone, infatti, la problematica di un possibile "abuso" dell'emergenza, in particolare quella terroristica, tramite un'enfatizzazione e strumentalizzazione delle paure e insicurezze sociali, nella ricerca di un consenso rispetto ad interventi volti a veicolare limiti alle libertà che poco o nulla hanno a che vedere con il fenomeno che formalmente si desidera contrastare.

Come già ricordato in altre sedi[22], si è, infatti, precisato che

> la prima emergenza, nella più generale emergenza del terrorismo, è proprio la difficile gestione dei suoi effetti emotivi, dal punto di vista sociale: il terrorismo evoca la militarizzazione dello strumento giuridi-

---

ciare ad una parte dei propri diritti ed alla libertà. Noi pensiamo che dobbiamo combattere la paura, certo dando sicurezze ai nostri cittadini, ma anche e soprattutto difendendo le nostre libertà democratiche e la convivenza tra culture. I nostri concittadini, su questi fronti, chiedono risposte concrete e non iniziative promozionali, finalizzate più ad accontentare i *mass media* ed a rassicurare l'opinione pubblica che non a proporre soluzioni concrete e reali» (T. BASILIO (M5S), *Resoconto stenografico della 399ª seduta n. 399 della camera di data 25 marzo 2015*, 74 s).

[20] Cfr. A. PECCIOLI, *Punibilità di atti preparatori alla realizzazione di condotte terroristiche: commento alle disposizioni di diritto penale sostanziale del d.l. 18 febbraio 2015, n. 7, conv. dalla l. 17 aprile 2015, n. 43*, in *Studium Iuris*, 2015, 771: «L'intervento del 2015 presenta le caratteristiche tipiche della legislazione dell'emergenza, in cui viene fatto un uso simbolico del diritto penale, mettendo in risalto il carattere imprescindibile ed esaustivo della risposta penale a fronte di pressanti esigenze di tutela della sicurezza sociale».

[21] E. MUSCO, *Consenso e legislazione penale*, in *Riv. it. dir. proc. pen.*, 1993, 88, il quale ci avverte del rischio che la legislazione penale possa divenire «una fabbrica di illusioni dentro la quale trovano insieme collocazione il popolo sciocco ed ignavo e gli attori del sistema politico».

[22] R. WENIN, *Disposizioni sull'addestramento…*, cit. in nota 13, 1893, contributo al quale sia consentito un richiamo anche per un'analisi più approfondita sul rapporto tra emergenza e consenso.

co-penale, l'esasperazione del diritto penale del nemico e spinge collettivamente a risposte di tipo eccezionale[23].

Una prima significativa differenza concerne lo scopo perseguito nello «sfruttamento» dell'emergenza, potendo esso consistere, come già ricordato, nell'introduzione di limitazioni alle libertà che in situazioni di normalità sarebbero mal tollerate[24], o anche nel rafforzamento politico del governo al potere, se non degli stessi Stati tramite la creazione verso l'esterno di un'immagine di forza ed efficienza:

> la fiducia moderna nei confronti del diritto e delle istituzioni politiche crolla e aumentano le paure: la razionalità cede all'irrazionalità. Incapaci di controllare fenomeni – fra cui il crimine globale – che, per definizione, sfuggono al proprio perimetro territoriale, i tradizionali poteri politici degli Stati-nazione – peraltro soggiogati alle stesse evanescenti forze economiche che muovono la globalizzazione – vedono minacciata la loro legittimazione e nell'intento di rifondare la propria autorità su un (facile) consenso scaturito dall'emotività e dal sentimento, gli Stati ostentano, spesso in modo spettacolare, complici anche i media, eccezionali esercizi dell'unico potere che la globalizzazione ha lasciato loro

[23] G.M. FLICK, *Dei diritti e delle paure*, in S. MOCCIA (a cura di), *op. cit.* in nota 18, 71.

[24] Cfr. E. LO MONTE, *Gli interventi in tema di misure di prevenzione: il problema del congelamento di beni*, in A.A. DALIA (a cura di), *op. cit.* in nota 2, 439: «il bisogno di tutela espresso dalla comunità si converte in domanda di pena. Il potere statuale assecondando tali spinte irrazionali amplia la portata del penalmente rilevante e vulnera, di fatto, gli spazi di libertà». Con riferimento al dibattito parlamentare in sede di conversione del d.l. 7/2015, si veda, oltre a quanto già riportato in nota 19, A. TOFALO (M5S), *Resoconto stenografico della 399ª seduta n. 399 della camera di data 25 marzo 2015*, 15, il quale osserva criticamente che «Questo decreto-legge è il risultato del modo con cui la legittima paura dei cittadini di fronte al gravissimo pericolo del terrorismo internazionale viene strumentalizzata per una propaganda mediatica populista che ha l'unico scopo di far accettare l'ennesimo decreto-legge sulle missioni italiane all'estero e il perseguimento di finalità celate che mirano alla repressione di condotte che nulla hanno a che fare con il terrorismo». Al contempo, come visto, è stata criticata la scelta di trattare in un unico provvedimento due tematiche distinte come la proroga delle missioni internazionali e l'introduzione di nuove previsioni normative.

intatto, l'uso della forza, nei confronti dei più disparati "nemici" di turno[25].

Un diverso profilo di indagine attiene al bene giuridico tutelato, in particolare ci si interroga circa l'eventuale legittimità del richiamo, a fondamento dell'intervento normativo, ad un "nuovo bene giuridico" da tutelare rappresentato per l'appunto dalla percezione di sicurezza nella collettività[26].

Poste tali premesse, ciò che preme analizzare in tale sede è l'idoneità del mezzo predisposto, da un punto di vista della tecnica legislativa adottata e della concreta operatività della norma incriminatrice – in particolare in materia di addestramento nell'uso di armi –, nel bilanciamento dei contrapposti diritti intaccati dallo strumento penale, forti dell'esperienza comparata e dell'analisi della normativa sovranazionale di riferimento.

La dimensione globale del fenomeno terroristico e la natura "adimensionale" delle nuove tecnologie hanno, infatti, reso sempre più pressante l'esigenza di una reazione a livello sovranazionale, innalzando organismi internazionali quali il Consiglio d'Europa[27], l'Unione eu-

[25] L. PASCULLI, *La normalizzazione della prevenzione eccezionale del crimine globale. Improvvisazione "con una mano legata" in quattro tempi e finale sull'emerso diritto della prevenzione criminale negativa*, in S. BONINI, L. BUSATTA, I. MARCHI (a cura di), *L'eccezione nel diritto. Atti della giornata di studio (Trento, 31 ottobre 2013)*, Trento, 2015, 325 s. Così facendo, ci dice l'autore, «Lo Stato governa con l'emergenza (e la paura)», *ibidem*.

[26] Cfr. sul punto A. CAVALIERE, *Può la 'sicurezza' costituire un bene giuridico o una funzione del diritto penale*, in *Critica del diritto*, 2009, 43 ss.; M. DONINI, *Sicurezza e diritto penale*, in *Cass. pen.*, 2008, 3559 ss. In generale sul rapporto tra sicurezza e diritto penale si veda anche M. DONINI, M. PAVARINI (a cura di), *Sicurezza e diritto penale*, Bologna, 2011. Con riferimento alla dottrina tedesca si vedano i contributi di K. GIERHAKE, *Der Zusammenhang von Freiheit, Sicherheit und Strafe im Recht. Eine Untersuchung zu den Grundlagen und Kriterien legitimer Terrorismusprävention*, Berlin, 2013 e R. VOIGT (a cura di), *Sicherheit versus Freiheit. Verteidigung der staatlichen Ordnung um jeden Preis?*, Wiesbaden, 2012, e letteratura ivi citata.

[27] È stato precisato, A. BERNARDI, *L'europeizzazione del diritto e della scienza penale*, Torino, 2004, 7 ss., che il processo di erosione del carattere meramente statuale dei sistemi penali europei e della relativa scienza tende a coincidere con la creazione del Consiglio d'Europa su impulso del quale sono state varate varie convenzioni (tra

ropea, l'Onu a protagonisti indiscussi di una nuova fase di contrasto. Al richiamato protagonismo si lega, peraltro, la critica circa un asserito *deficit* di legittimazione democratica che caratterizzerebbe tali organi[28].

Il percorso verso una progressiva armonizzazione delle legislazioni nazionali, che pare rappresentare il presupposto indefettibile per un'efficace strategia di contrasto, impone a nostro avviso l'adozione di un metodo comparato[29] che consenta di cogliere il reale contenuto delle modifiche normative, frutto troppo spesso, come visto, di frenesie interventiste legate all'emotività del momento.

In tale ottica non si può celare la critica che occorre muovere al ricorso alla decretazione d'urgenza quale ordinario criterio di intervento normativo[30]: che dei diritti e delle libertà dei cittadini, intaccati dallo

---

cui, come si vedrà, quella di Varsavia del 2005 sulla prevenzione del terrorismo). Si tratta di atti che non si limitano a predisporre strumenti giuridici di cooperazione, ma spesso sono diretti ad armonizzare gli ordinamenti penali, al fine di riavvicinare, finanche uniformare, le risposte date dalle legislazioni nazionali a taluni fenomeni criminali.

[28] La critica si è rivolta per lo più alle risoluzioni emanate dalle Nazioni Unite, in particolare dal Consiglio di Sicurezza sulla base del capitolo VII della Carta: cfr. J. MACKE, *UN-Sicherheitsrat und Strafrecht. Legitimation und Grenzen einer internationalen Strafgesetzgebung*, Berlin, 2010, *passim*; F. RAUTENBERG, *Rechtsstaatswidriges Feindstrafrecht oder notwendige Maßnahmen zur Terrorismusbekämpfung? Zur Verfassungsmäßigkeit der §§ 89a, 89b und 91 StGB*, Baden-Baden, 2014, 53 ss. Si è fatto a riguardo riferimento ad una procedura normativa definita «a cascata» che in attuazione delle risoluzioni adottate in seno alle Nazioni Unite ha visto l'emanazione di atti comunitari, quali decisioni quadro e regolamenti, a loro volta destinati ad essere applicati su base nazionale: cfr. V. MASARONE, *Politica criminale e diritto penale nel contrasto al terrorismo internazionale. Tra normativa interna, europea ed internazionale*, Napoli, 2013, 135. Rispetto all'UE si veda C. GRANDI, *Il ruolo del Parlamento europeo nell'approvazione delle direttive di armonizzazione penale*, in *Riv. it. dir. proc. pen.*, 2015, 678 ss. e bibliografia ivi citata, in particolare p. 671, nota 5.

[29] Sul ruolo del metodo comparato ai fini di una reale armonizzazione: F. PALAZZO, M. PAPA, *Lezioni di diritto penale comparato*, 3ª ed., Torino, 2013, 33 ss.

[30] Si pensi solo alle recenti esperienze legate ad esempio al c.d. decreto Pisanu, d.l. n. 144, del 27 luglio 2005 («Misure urgenti per il contrasto del terrorismo internazionale»), emanato dopo gli attentati di Londra e convertito con l. 31 luglio 2005 n. 155, ossia a pochi giorni dalla sua emanazione, o al d.l. n. 7 del 18 febbraio 2015 («Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle

strumento penale, debba disporre, di fatto, in via ordinaria il potere esecutivo, come è stato acutamente osservato, rappresenta una situazione di "anormalità" politica e culturale, che si pone in spregio allo spirito della Costituzione[31].

In sintesi lo scopo del presente scritto è di far emergere la profonda delicatezza del tema affrontato, dando un rinnovato stimolo alla riflessione critica e scientifica, ed evidenziare l'utilità del metodo comparato nella lettura delle norme di derivazione sovranazionale. Nel fare ciò si prenderanno precipuamente a riferimento le norme dettate in materia di addestramento nell'uso di armi.

## *2. Normativa sovranazionale di riferimento*

Nel 2005 il Consiglio d'Europa adottò a Varsavia la convenzione per la prevenzione del terrorismo, CETS n. 196. La convenzione si poneva lo scopo di accrescere l'efficacia degli strumenti internazionali già esistenti in materia di lotta al terrorismo. Il testo era destinato a intensificare gli sforzi degli Stati membri nella prevenzione del terrorismo.

---

iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione»), convertito con l. 17 aprile 2015, n. 43, dopo essere stato «blindato» dagli emendamenti con il voto di fiducia al Senato, considerato che un'eventuale modifica non avrebbe consentito di rispettare i tempi tecnici per la conversione.

[31] E. MUSCO, *Consenso e legislazione penale*, in *Riv. it. dir. proc. pen.*, 1993, 86. Aspetto su cui peraltro si è incentrata la critica dell'opposizione in sede di conversione del decreto legge 7/2015 cfr. *Resoconto stenografico della 399ª seduta n. 399 della camera di data 25 marzo 2015* e *Resoconto stenografico della seduta n. 428 del Senato di data 14 aprile 2015.* Si è peraltro evidenziata l'opportunità di una riforma strutturale ispirata a ragioni di razionalità pratica: G. LOSAPPIO, *Diritto penale del nemico, diritto penale dell'amico, nemici del diritto penale*, in A. GAMBERINI, R. ORLANDI (a cura di), *Delitto politico e diritto penale del nemico*, Bologna, 2007, 262 s., il quale sottolinea come alla luce di assemblee parlamentari spesso soggiogate dalla volontà del governo e al susseguente scemare del significato di garanzia del principio di legalità, non basterebbe più il mero rifiuto di annoverare il decreto legge e decreto legislativo tra le fonti del diritto penale, ma si imporrebbe l'acquisto di una razionalità pratica che si confronti con i limiti dei disegni costituzionali del secondo dopoguerra. Sul tema in generale si veda: C. CUPELLI, *La legalità delegata. Crisi e attualità della riserva di legge nel diritto penale*, Napoli, 2012.

Erano indicate due modalità di azione per il conseguimento dell'obiettivo prefissato: da un lato l'introduzione di nuove fattispecie penali volte a sanzionare l'istigazione a commettere reati terroristici, il reclutamento e l'addestramento a fini terroristici, dall'altro il consolidamento e rafforzamento della cooperazione in materia di prevenzione, sia a livello nazionale (politiche nazionali di prevenzione), che internazionale (modifica degli accordi di estradizione e di mutua assistenza e di ogni altro mezzo esistente)[32]. La convenzione fu firmata anche dall'Italia nel 2005 e la legge di autorizzazione alla ratifica fu emanata nel 2016[33].

[32] «The Convention purports to achieve this objective, on the one hand, by establishing as criminal offences certain acts that may lead to the commission of terrorist offences, namely: public provocation, recruitment and training and, on the other hand, by reinforcing co-operation on prevention both internally, in the context of the definition of national prevention policies, and internationally through a number of measures, inter alia, by means of supplementing and, where necessary, modifying existing extradition and mutual assistance arrangements concluded between Parties and providing for additional means, such as spontaneous information, together with obligations relating to law enforcement, such as the duty to investigate, obligations relating to sanctions and measures, the liability of legal entities in addition to that of individuals, and the obligation to prosecute where extradition is refused» (Rapporto esplicativo, 4, par. 26, disponibile sul sito *www.coe.int*).

[33] Prima della l. 28 luglio 2016, n. 153 (Norme per il contrasto al terrorismo, nonché ratifica ed esecuzione: a) della Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, fatta a Varsavia il 16 maggio 2005; b) della Convenzione internazionale per la soppressione di atti di terrorismo nucleare, fatta a New York il 14 settembre 2005; c) del Protocollo di Emendamento alla Convenzione europea per la repressione del terrorismo, fatto a Strasburgo il 15 maggio 2003; d) della Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo, fatta a Varsavia il 16 maggio 2005; e) del Protocollo addizionale alla Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, fatto a Riga il 22 ottobre 2015) vi furono vari progetti di legge di ratifica ed esecuzione della Convenzione, nonché di adeguamento dell'ordinamento italiano; in particolare uno presentato durante la XV legislatura (S. 1799) e un altro, che riprendeva l'articolato e la relazione del precedente progetto, durante la XVI legislatura (S. 852); entrambi, così come il progetto C. 1789, presentato anch'esso durante la XVI legislatura, furono frustrati dalla conclusione anticipata delle legislature. La l. 153/2016 prevede tra l'altro all'art. 4 delle modifiche al codice penale con l'introduzione di nuove fattispecie incriminatrici. A commento della legge si veda F. FASANI, *Un nuovo intervento di contrasto al terrorismo internazionale*, in *Dir. pen. proc.*, 2016, 1555 ss.

La Convenzione di Varsavia all'art. 7 definisce l'addestramento per finalità di terrorismo come l'atto di fornire istruzioni per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose ovvero altre tecniche o metodi specifici al fine di commettere un reato terroristico – sottolineo – nella consapevolezza che le istruzioni impartite sono intese per conseguire tale obiettivo[34]. La consapevolezza dell'utilizzo delle istruzioni impartite, come sarà precisato meglio nel prosieguo, rappresenta, infatti, un requisito della fattispecie di particolare rilievo ai fini della selezione del disvalore di condotte che rischiano di essere socialmente neutre.

La richiamata previsione fu ripresa, con alcune parziali e minime modifiche, dalla decisione quadro del Consiglio dell'Unione europea del 28 novembre 2008 (2008/919/GAI) che modificava, per quanto qui rileva, l'art. 3, reati connessi alle attività terroristiche, della decisione quadro del 13 giugno 2002 (2002/475/GAI)[35].

Per quanto concerne gli antecedenti, per così dire "storici", la fattispecie, salva l'espressa finalità di terrorismo e l'estensione dell'oggetto dell'addestramento e della punibilità all'addestrato, riprende nella struttura la sezione quindicesima della normativa emergenziale per l'Irlanda del nord del 1975[36]. La previsione fu poi estesa a tutto il Regno Unito[37]

[34] Article 7 – Training for terrorism.

For the purposes of this Convention, "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence, knowing that the skills provided are intended to be used for this purpose.

[35] Articolo 3 Reati connessi ad attività terroristiche.

1. Ai fini della presente decisione quadro, si intende per: […]

c) "addestramento a fini terroristici" l'atto di fornire istruzioni per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose ovvero altre tecniche o metodi specifici al fine di commettere uno dei reati di cui all'articolo 1, paragrafo 1, lettere da a) a h), nella consapevolezza che le istruzioni impartite sono intese per conseguire tale obiettivo.

Sull'attuazione della decisione negli Stati membri si veda la relazione della Commissione del 5.09.2014, COM(2014) 554 final.

[36] Northern Ireland (Emergency Provisions) (Amendment) Act 1975

15 Training in making or use of firearms, explosives or explosive substances.

con il *terrorism act* del 2000[38] e nel 2006 a quest'ultima norma fu affiancata la disposizione che sanziona espressamente l'addestramento per finalità di terrorismo[39].

I recenti gravi fatti di terrorismo hanno ulteriormente "sollecitato" la comunità internazionale; vanno in tale senso menzionate – salvo un più puntuale approfondimento di singole previsioni nel prosieguo della trattazione – le Risoluzioni del consiglio di sicurezza dell'Onu n. 2170, 2178 e 2195 del 2014, 2199, 2214, 2249 e 2255 del 2015, il protocollo addizionale alla convenzione di Varsavia sul terrorismo di Riga del 22

---

(1) Subject to subsection (2) below, any person who instructs or trains another or receives instruction or training in the making or use of firearms, explosives or explosive substances shall be liable–
(a) on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding £400, or both;
(b) on conviction on indictment to imprisonment for a term not exceeding five years or to a fine, or both.
(2) In any prosecution for an offence under this section it shall be a defence for the person charged to prove that the instruction or training was given or received with lawful authority or for industrial, agricultural or sporting purposes only or otherwise with good reason…

Per un'analisi, anche dell'evoluzione storica, della normativa in materia di terrorismo nell'Irlanda del Nord si veda J. BLACKBOURN, *Anti-Terrorism Law and Normalising Northern Ireland*, London, 2015.

[37] La previsione fu ripresa nonostante il parere contrario di Lord Lloyd of Berwick, chiamato a valutare l'opportunità di estendere la previsione – al tempo contenuta nell'EPA (*Northern Ireland Emergency Provisions Act*) del 1996 – a tutto il Regno Unito. L'opinione negativa si fondava sull'ampia diffusione, in particolare in internet, delle informazioni in oggetto, delle difficoltà probatorie e della conseguente scarsa applicazione della norma (LORD LLOYD OF BERWICK, *Inquiry into Legislation Against Terrorism - Command Paper No. 3420*, vol. 1, London, 1996, 95). Ad avviso di alcuni commentatori i motivi che spinsero a disattendere le raccomandazioni di Lord Lloyd of Berwick potrebbero rinvenirsi in un fatto storico, gli attentati a sfondo razzista e omofobo posti in essere nel 1999 a Londra da David Copeland, il quale aveva reperito le informazioni per la costruzione degli ordigni utilizzati su internet (cfr. C. WALKER, *Terrorism and the Law*, Oxford, 2011, 205; ID., *Blackstone's Guide to the Anti-terrorism Legislation*, 2ª ed., Oxford, 2009, 182).

[38] Terrorism Act 2000, 54 Weapons training.

[39] Terrorism Act 2006, 6 Training for terrorism.

ottobre 2015[40] e la proposta di direttiva del Parlamento europeo e del Consiglio sulla lotta contro il terrorismo, che dovrebbe sostituire la decisione quadro del Consiglio 2002/475/GAI sulla lotta contro il terrorismo[41].

Sia il protocollo addizionale di Riga[42], sia la proposta di direttiva[43] – che di fatto ricalca il primo[44] – intervengono sulla disciplina della con-

[40] Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, CETS n. 217, la cui entrata in vigore, ai sensi dell'art. 10, è prevista dopo la sesta ratifica. Il primo Stato a ratificare il protocollo addizionale fu l'Albania. Il testo è disponibile sul sito *www.coe.int*.

[41] Il testo della proposta è disponibile sul sito dell'Unione europea *www.eur-lex.europa.eu*.

[42] Article 3 – Receiving training for terrorism.

1 For the purpose of this Protocol, "receiving training for terrorism" means to receive instruction, including obtaining knowledge or practical skills, from another person in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence.

2 Each Party shall adopt such measures as may be necessary to establish "receiving training for terrorism", as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

[43] In tal caso opportunamente si provvede a disciplinare in maniera differenziata, in conformità a talune esperienze nazionali (es. Germania, Austria), la condotta di addestramento attivo e quella di addestramento passivo.

Articolo 7 Atto di impartire un addestramento a fini terroristici.

Gli Stati membri adottano le misure necessarie per assicurare che costituisca reato, se compiuto intenzionalmente, l'atto di impartire istruzioni per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose ovvero altre tecniche o metodi specifici al fine di commettere o contribuire a commettere uno dei reati di cui all'articolo 3, paragrafo 2, lettere da a) ad h), nella consapevolezza che le competenze trasmesse sono destinate ad essere utilizzate a tale scopo.

Articolo 8 Atto di ricevere un addestramento a fini terroristici.

Gli Stati membri adottano le misure necessarie per assicurare che costituisca reato, se compiuto intenzionalmente, l'atto di ricevere istruzioni da un'altra persona per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose ovvero altre tecniche o metodi specifici al fine di commettere o di contribuire alla commissione di uno dei reati di cui all'articolo 3, paragrafo 2, lettere da a) ad h).

[44] La convenzione di Varsavia e il protocollo addizionale furono firmati dall'UE il 22 ottobre 2015.

dotta di addestramento, andando a sanzionare l'etero-addestramento passivo e prevedendo come mera facoltà la punizione da parte degli Stati anche di forme di addestramento autonomo. La scelta di sanzionare anche l'addestrato pare poggiare sulle indicazioni del "Group of Parties" del Consiglio di Europa che monitora l'implementazione della convenzione sulla prevenzione del terrorismo; muovendo dalla frequente incriminazione dell'addestramento passivo – così anche in Italia –, si concludeva per la possibile utilità della stessa nell'ottica del contrasto del terrorismo, invocando pertanto un approfondimento della tematica da parte del comitato degli esperti (Codexter)[45]. L'indicazione fu poi per l'appunto recepita dal Codexter in occasione del 27° incontro plenario tenutosi il 13-14 novembre 2014, confluendo infine nel protocollo addizionale.

Si precisa nelle relazioni esplicative che l'addestramento sanzionato richiede una partecipazione attiva[46], nondimeno, gli «Stati membri pos-

[45] «In this regard, the Group of Parties finds that the fact that a large majority of the responding States Parties have, in one or another way, already criminalised or are considering criminalising the receiving of training at national level is an important indicator that such criminalisation is also called for at the international level in order to further enhance international cooperation to prevent and combat terrorism. Hence the Group of Parties wishes to refer the question of criminalisation of the receiving of training for terrorism to CODEXTER for a more in depth examination, taking into account the various arguments pro et contra, which have been put forward by the responding States Parties», *Summary of the Thematic Assessment Report on the implementation of Article 7 "Training for terrorism" Council of Europe Convention on the Prevention of Terrorism (CETS No 196)*, del 17.07.2014, 4, disponibile sul sito *www.coe.int/gmt*.

[46] Si tratta, come si vedrà, di un requisito strutturale elaborato in particolare dalla dottrina tedesca e austriaca. Cfr. per l'Austria: F. PLÖCHL, *§ 278e Ausbildung für terroristische Zwecke*, in F. HÖPFEL, E. RATZ (a cura di), *Wiener Kommentar zum Strafgesetzbuch*, 100. Lfg. (Jänner 2014), 2ª ed., Wien, 2014, 92; per la Germania si veda: C. BECKER, J. STEINMETZ, *§ 89a Vorbereitung einer schweren staatsgefährdenden Gewalttat*, in H. MATT, J. RENZIKOWSKI, *Strafgesetzbuch Kommentar*, München, 2013, 946; T. FISCHER, *§ 89a Vorbereitung einer schweren staatsgefährdenden Gewalttat*, in ID., *Strafgesetzbuch mit Nebengesetzen*, 62ª ed., München, 2015; N. GAZEAS, *§ 89a Vorbereitung einer schweren staatsgefährdenden Gewalttat*, in K. LEIPOLD, M. TSAMBIKAKIS, M.A. ZÖLLER (a cura di), *AnwaltKommentar StGB*, Bonn, 2011, 752; H.-U. PAEFFGEN, *§ 89a Vorbereitung einer schweren staatsgefährdenden Gewalttat*, in U. KINDHÄUSER, U. NEUMANN, H.-U. PAEFFGEN (a cura di), *Strafgesetzbuch*, 4ª ed., 2013, Baden-Baden, 218; J. SCHÄFER, *§ 89a Vorbereitung einer schweren staatsgefähr-*

sono decidere di considerare reato nel loro ordinamento interno forme di "autoapprendimento"»[47].

I due strumenti normativi richiamati prevedono poi la punibilità del tentativo per quanto concerne la condotta attiva (addestratore), mentre introducono una mera possibilità in relazione alla punizione del tentativo rispetto al soggetto passivo dell'addestramento[48]. A differenza del protocollo addizionale, in cui si configura come mera possibilità[49], nella proposta di direttiva si introduce un obbligo di incriminazione del concorso nell'addestramento passivo[50].

---

*denden Gewalttat*, in W. JOECKS, K. MIEBACH (a cura di), *Münchener Kommentar zum Strafgesetzbuch. III. §§ 80-184g StGB*, 2ª ed., München, 2012, 125; D. STERNBERG- LIEBEN, *§ 89a Vorbereitung einer schweren staatsgefährdenden Gewalttat*, in A. SCHÖNKE, H. SCHRÖDER, *Strafgesetzbuch Kommentar*, 29ª ed., 2014, München, 1351; M.A. ZÖLLER, *§ 89a Vorbereitung einer schweren staatsgefährdenden Gewalttat*, J. WOLTER (a cura di), *Systematischer Kommentar zum Strafgesetzbuch. II. §§ 46-122 StGB*, 8ª ed., 2012, Köln, 25.

[47] Relazione sulla proposta di direttiva del parlamento europeo e del consiglio sulla lotta contro il terrorismo e che sostituisce la decisione quadro del Consiglio 2002/475/GAI sulla lotta contro il terrorismo, 18. La relazione riprende in tal punto pedissequamente il rapporto esplicativo del protocollo addizionale della convenzione di Varsavia, 6, par. 40: «The perpetrator must normally take an active part in the training. An example would be the participation of the perpetrator in interactive training sessions via the Internet. Parties may choose to criminalise forms of "self-study" in their domestic law».

[48] «The drafters did not consider it necessary to criminalise the attempt or the aiding or abetting of this offence, cf. also Article 9 of the Protocol. Parties are however free to do so, if they consider it appropriate in their domestic legal systems» (Rapporto esplicativo, 4, par. 42). Mentre per quanto concerne la proposta di direttiva, l'art. 8 (atto di ricevere un addestramento) non è tra quelli per i quali l'art. 16 prevede la punibilità del tentativo.

[49] Cfr. nota 48.

[50] «In aggiunta alle condizioni attualmente definite all'articolo 4 della decisione quadro 2002/475/GAI, modificata dalla decisione quadro 2008/919/GAI, si propone di perseguire penalmente anche il concorso in relazione all'atto di ricevere un addestramento. Mentre ciò non è previsto ai sensi del Protocollo addizionale, perseguire penalmente tali attività è coerente con il fatto di qualificare come reato il concorso in relazione ad altre attività preparatorie. Aiutare una persona a ottenere istruzioni (per esempio traducendo contenuti terroristici in una lingua straniera in piena consapevolezza del contenuto e dell'impiego previsto di tali istruzioni) non è di fatto meno riprovevole dell'offrire un analogo sostegno (traduzione) a una persona che impartisce un addestramento» (Relazione sulla proposta di direttiva, 20).

Riportate sinteticamente le previsioni sovranazionali, si passerà ora all'analisi delle disposizioni italiane in un confronto con le esperienze straniere.

### *3. La previsione normativa italiana in materia di addestramento per finalità di terrorismo*

Nel 2005, a seguito dei gravi fatti di terrorismo avvenuti a Londra e in Spagna, il legislatore italiano, dando seguito a quanto previsto dalla Convezione di Varsavia, con il decreto legge Pisanu, d.l. n. 144, del 27 luglio 2005, introdusse nel codice penale fra l'altro l'art. 270-*quinquies* c.p. Tale previsione normativa sanziona per l'appunto l'addestramento per finalità di terrorismo. Originariamente l'articolo in commento disponeva:

> Chiunque, al di fuori dei casi di cui all'articolo 270-bis, addestra o comunque fornisce istruzioni sulla preparazione o sull'uso di materiali esplosivi, di armi da fuoco o di altre armi, di sostanze chimiche o batteriologiche nocive o pericolose, nonché di ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo, anche se rivolti contro uno Stato estero, un'istituzione o un organismo internazionale, è punito con la reclusione da cinque a dieci anni. La stessa pena si applica nei confronti della persona addestrata.

La norma fu modificata nel 2015, a seguito dei fatti di terrorismo avvenuti in Francia, con il d.l. 18 febbraio 2015, n. 7, convertito con modifiche dalla l. 17 aprile 2015, n. 43[51]. Con tale intervento normativo

[51] A commento della modifica normativa si veda: AA.VV., *Commento al decreto legge 7/2015 convertito in legge n. 43/2015*, in *La legislazione penale*, disponibile *online* sul sito *www.lalegislazionepenale.eu*; F. BATTAGLIA, *L'attività legislativa italiana di recepimento degli obblighi internazionali in materia di lotta al terrorismo internazionale e combattenti stranieri*, in *Federalismi.it Rivista di diritto pubblico italiano, comunitario e comparato*, 2015, n. 4; M. CAPUTO, *Tra viaggi e miraggi: l'impatto sul codice penale delle nuove fattispecie antiterrorismo*, in G.M. BACCARI, K. LA REGINA, E.M. MANCUSO (a cura di), *Il nuovo volto della giustizia penale*, Padova, 2015, 77 ss.; P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa*

si estese la punibilità all'"auto-addestramento" e si introdusse una circostanza aggravante per l'utilizzo di strumenti informatici, stabilendosi che

> La stessa pena si applica nei confronti della persona addestrata, nonché della persona che avendo acquisito, anche autonomamente, le istruzioni per il compimento degli atti di cui al primo periodo, pone in essere comportamenti univocamente finalizzati alla commissione delle condotte di cui all'articolo 270-sexies. Le pene previste dal presente articolo sono aumentate se il fatto di chi addestra o istruisce è commesso attraverso strumenti informatici o telematici.

---

*antiterrorismo*, in *Arch. pen. web.*, 2016, n. 1; A. CAVALIERE, *Considerazioni critiche intorno al d.l. antiterrorismo n. 7 del 18 febbraio 2015*, in *Dir. pen. cont.*, 31 marzo 2015; S. COLAIOCCO, *Prime osservazioni sulle nuove fattispecie antiterrorismo introdotte dal decreto-legge n. 7 del 2015*, in *Arch. pen. web.*, 2015, n. 1; ID., *Le nuove norme antiterrorismo e le libertà della persona: quale equilibrio?*, in *Arch. pen. web.*, 2015, n. 2; A. CONZ, L. LEVITA, *Antiterrorismo. Commento organico al D.L. 18 febbraio 2015, n. 7, convertito in L. 17 aprile 2015, n. 43*, Roma, 2015; M.F. CORTESI, *Il nuovo sistema di prevenzione del "terrorismo"*, G.M. BACCARI, K. LA REGINA, E.M. MANCUSO (a cura di), *op. cit.* in questa nota, 159 ss.; M.F. CORTESI, *I riflessi sul sistema processuale, penitenziario e di prevenzione*, in *Dir. pen. proc.*, 2015, 947 ss.; F. FASANI, *Le nuove fattispecie antiterrorismo: una prima lettura*, in *Dir. pen. proc.*, 2015, 926 ss.; R.E. KOSTORIS, F. VIGANÒ (a cura di), *op. cit.* in nota 14; G. LEO, *Nuove norme in materia di terrorismo. Voce Libro dell'anno del Diritto Treccani 2016*, 2016, disponibile sul sito *www.treccani.it/enciclopedia/nuove-norme-in-materia-di-terrorismo_(Il-Libro–dell'anno-del-Diritto)*, pubblicata anche su *www.penalecontemporaneo.it*; C.D. LEOTTA, *La repressione penale del terrorismo a un anno dalla riforma del D.L. 18 febbraio 2015, n. 7, conv. con modif. dalla L. 17 aprile 2015, n. 43*, in *Arch. pen. web.*, 2016, n. 1; G. MARINO, *Il sistema antiterrorismo alla luce della L. 43/2015: un esempio di "diritto penale del nemico"?*, in *Riv. it. dir. proc. pen.*, 2016, 1388 ss.; U. NAZZARO, *Le misure di contrasto al terrorismo internazionale alla luce della legge 17 aprile 2015*, n. 43, in *Riv. pen.*, 2015, 10, 822 ss.; A. PECCIOLI, *op. cit.* in nota 20, 770 ss.; L. STAFFLER, *op. cit.* in nota 2; A.P. VIOLA, *Le nuove misure investigative, processuali e ordinamentali per il contrasto al terrorismo*, in G.M. BACCARI, K. LA REGINA, E.M. MANCUSO (a cura di), *op. cit.* in questa nota, 117 ss.; R. WENIN, *L'addestramento per finalità di terrorismo alla luce delle novità introdotte dal d.l. 7/2015. Una riflessione comparata sulle tecniche di descrizione della fattispecie muovendo dalla sentenza del Bundesgerichtshof tedesco StR 243*/13, in *Dir. pen. cont.*, 3 aprile 2015.

Si è infine prevista la pena accessoria della perdita della potestà genitoriale laddove sia coinvolto un minore.

L'intento dichiarato dal legislatore italiano era di adeguare l'ordinamento italiano alla risoluzione ONU n. 2178 "innestando" una

> nuova fattispecie di reato che rende punibile anche l'auto-addestramento, cioè la condotta di chi si prepara al compimento di atti di terrorismo, attraverso una ricerca e un apprendimento individuali e autonomi delle "tecniche" necessarie a perpetrare simili atti. […] In tal modo viene estesa l'area della punibilità anche ai terroristi che operano sganciati da sodalizi e da organizzazioni (cosiddetto lupo solitario)[52].

Vi sarà poi modo di soffermarsi in punto corrispondenza tra intenti dichiarati e portata effettiva delle modifiche introdotte.

Con riferimento all'addestramento nell'uso di armi, va menzionato come accanto all'art. 270-*quinquies* il legislatore italiano con il decreto legge Pisanu introdusse nel nostro ordinamento anche l'art. 2-*bis* nella l. 895 del 1967, che detta «disposizioni per il controllo delle armi». Tale norma stabilisce:

> Chiunque fuori dei casi consentiti da disposizioni di legge o di regolamento addestra taluno o fornisce istruzioni in qualsiasi forma, anche anonima, o per via telematica sulla preparazione o sull'uso di materiali esplosivi, di armi da guerra, di aggressivi chimici o di sostanze batteriologiche nocive o pericolose e di altri congegni micidiali è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a sei anni[53].

L'art. 270-*quinquies* c.p. e l'art. 2-*bis* differiscono essenzialmente per l'oggetto dell'addestramento e dell'istruzione e per l'elemento soggettivo[54] richiesto per la fattispecie prevista dal codice penale[55]. Tra le

[52] Disegno di legge di conversione (C. 2893), 6.

[53] Scopo della previsione era di calibrare «la fattispecie e la relativa sanzione con il disposto degli articoli 1, 2 e 5 della legge 2 ottobre 1967, n. 895, riguardante le armi da guerra, quelle chimiche e batteriologiche e gli altri congegni micidiali», disegno di legge di conversione (S. 3571), 7.

[54] Mentre nel caso dell'art. 2-*bis* l. 895/1967 la fattispecie è a dolo generico, nel caso dell'art. 270-*quinquies* c.p. l'orientamento maggioritario in dottrina e giurisprudenza richiede un doppio dolo specifico, dato dalla volontà di compiere atti di violenza o di

due norme sussiste un rapporto di reciproca specialità[56] nel senso che la condotta tipica dell'art. 270-*quinquies* è più ampia, ricomprendendo qualsiasi arma da fuoco[57], mentre rispetto all'elemento soggettivo l'art. 2-*bis* ricomprende condotte non punite dalla norma del codice penale, prescindendo esso, infatti, dall'esistenza di uno scopo specifico nell'attività di addestramento o istruzione. In altre parole, il disvalore della condotta, assorbito nell'art. 270-*quinquies* dal fine che deve guidare la stessa, sarebbe incentrato nell'art. 2-*bis* dall'oggettiva pericolosità della condotta, data dall'oggetto al quale si riferiscono le istruzioni[58].

Illustrato brevemente il dato normativo, ci si soffermerà sull'utilità del metodo comparato nella lettura della norma nazionale di derivazione sovranazionale.

---

sabotaggio di servizi pubblici essenziali e dalla finalità di terrorismo, che trova definizione, come noto, nell'art. 270-*sexies* c.p. Cfr. L. SCOTTO, *Commento sub art. 8, D.L. 27.7.2005 n. 144*, in *LP*, 2005, 494.

[55] Per un approfondimento del rapporto tra le due norme si rinvia, anche per i necessari riferimenti bibliografici, a R. WENIN, *Disposizioni sull'addestramento…*, cit. in nota 13, 1893 ss.; ID., *La strumentalizzazione della logica "amico-nemico" nel rovesciamento del rapporto "eccezione (illiceità)-regola (liceità)"? Alcuni spunti di riflessione sulla tenuta del sistema, muovendo dalle disposizioni sull'addestramento nell'uso di armi*, in S. BONINI, L. BUSATTA, I. MARCHI (a cura di), *op. cit.* in nota 25, 293 ss.

[56] Cfr. G. CIVELLO, *Armi ed esplosivi. L. 2.10.1967, n. 895*, in M. RONCO, S. ARDIZZONE (a cura di), *Codice penale ipertestuale. Leggi complementari*, Milano, 2007, 221. Si veda anche C. PIEMONTESE, Sub *Art. 270*-quinquies, in T. PADOVANI (a cura di), *Codice penale commentato*, tomo I, 6ª ed., 2014, Milano, 1554, laddove l'autore evidenzia come il legislatore abbia provveduto ad escludere il concorso fra le due norme mediante una clausola di riserva, quella del «salvo che il fatto costituisca più grave reato» di cui all'art. 2-*bis*, «suscettibile di far emergere il significato specializzante della proiezione finalistica della condotta prevista nell'art. 270-*quinquies* c.p.» e S. REITANO, *Riflessioni in margine alle nuove fattispecie antiterrorismo*, in *Riv. it. dir. proc. pen.*, 2007, 252 ss.

[57] L. PISTORELLI, *op. cit.* in nota 18, 56.

[58] Cfr. L. SCOTTO, *op. cit.* in nota 54, 496. Si tratta di uno schema che si ritrova anche in altre esperienze straniere; così ad esempio, come già ricordato, nel Regno Unito (*Terrorism Act* 2000, 54 *Weapons training*; *Terrorism Act* 2006, 6 *Training for terrorism*), in Germania (§ 89a, StGB *Vorbereitung einer schweren staatsgefährdenden Gewalttat*; *Waffengesetz* (WaffG) § 40 *Verbotene Waffen*).

*4. La condotta del fornire istruzioni e dell'addestramento*

Innanzitutto preme rilevare che mentre le norme sovranazionali definiscono il fornire istruzioni come una modalità attraverso cui si realizza l'addestramento, la norma italiana[59] parrebbe attribuire alla condotta istruttiva autonoma rilevanza penale facendola peraltro confluire con l'addestramento in un'unica norma incriminatrice[60]. Ciò ha dato luogo ad una serie di difficoltà interpretative di assoluto rilievo.

Va ricordato che originariamente la Convenzione di Varsavia non prevedeva la punibilità del soggetto passivo. La punibilità di quest'ultimo è invece ora prevista dal protocollo addizionale. Il legislatore italiano, al pari di altri legislatori stranieri[61], anticipò dunque le scelte incriminatrici sovranazionali[62].

L'estensione della punibilità al soggetto passivo dell'addestramento fu peraltro oggetto di critica in seno alla dottrina italiana. All'uopo si è evidenziato come in realtà si finisca per punire una mera pericolosità soggettiva, non potendosi condividere l'affermazione secondo cui l'offesa sarebbe insita non nel soggetto, ma nell'addestramento che egli avrebbe ricevuto[63].

La scelta di distinguere tra addestramento ed istruzione e di punire inizialmente solo il soggetto addestrato, ha impegnato la dottrina e giurisprudenza nel difficile compito di individuare un criterio discretivo tra tali due condotte.

---

[59] Così anche in altre esperienze nazionali: Regno Unito, Germania, Austria. Queste ultime (§ 278f StGB austriaco e § 91 StGB tedesco), tuttavia, fanno riferimento alla diffusione di informazioni e la punizione è subordinata alla circostanza che la condotta, per le modalità di realizzazione, sia idonea ad istigare alla commissione di un reato terroristico.

[60] Il condizionale è giustificato dal fatto che secondo taluna dottrina, come si vedrà meglio nel prosieguo, l'istruzione non sarebbe altro che una specificazione della condotta di addestramento; cfr. nota 64.

[61] Cfr. Regno Unito, Germania, Austria, Francia, Australia, ecc. Sul punto si veda anche la relazione della Commissione europea del 5.09.2014, COM(2014) 554 final, 9.

[62] Cfr. F. ROBERTI, *op. cit.* in nota 2, 532.

[63] M. DONINI, *Lo* status *di terrorista: tra il nemico e il criminale. I diritti fondamentali e la giurisdizione penale come garanzia contro, o come giustificazione per l'uso del diritto come arma?*, in S. MOCCIA (a cura), *op. cit.* in nota 18, 99.

Secondo un primo orientamento in realtà non ci si troverebbe di fronte a condotte alternative: il fornire istruzioni, infatti, non rappresenterebbe "altro" rispetto all'addestramento, ma solo il contenuto più tipico[64].

L'orientamento maggioritario ritiene viceversa che le due condotte debbano essere distinte sia per motivi criminologici, sia in ragione della costruzione normativa[65].

L'elemento differenziale che si è ritenuto di poter individuare si fonda sull'esistenza di un rapporto intersoggettivo tra addestrato e addestratore, non richiesto viceversa nel caso della diffusione di istruzioni che potrebbe quindi avvenire anche *ad incertam personam*. L'accento viene posto o sulla «ripetitività» dei contatti – intensità, reciprocità e interazione fra soggetti – che qualificherebbe l'addestramento rispetto al fornire istruzioni, caratterizzato da mera occasionalità, o sull'esistenza di un contatto diretto e di reciproca conoscenza rispetto a soggetti determinati che invece mancherebbe nel caso del fornire istruzioni[66].

---

[64] A. VALSECCHI, *Brevi osservazioni*, cit. in nota 18, 1228; G. PADOVANI, Commento *all'art. 15 d.l. 27.07.05 n. 144*, in *La legislazione penale*, 2005, 562. Seguendo una siffatta lettura si potrebbe sostenere, come ci ricorda a livello di ipotesi D. FALCINELLI, *L'atto dispositivo nei delitti contro il patrimonio. Sezioni e intersezioni del sistema penale*, Torino, 2013, 84 ss., che la disgiunzione («o comunque») eretta tra le condotte possa leggersi come il frammezzo di una endiadi, e la successiva unificazione della terminologia linguistica occorsa con l'uso della sola espressione «persona addestrata» non impedirebbe quindi di leggere nella punibilità dell'addestrato anche la punibilità del recettore di nozioni; soluzione che per evidenti ragioni, non ci sentiamo di condividere.

[65] Una conferma in tal senso si potrebbe ricavare anche dalla formulazione della nuova aggravante introdotta nel 2015: «Le pene previste dal presente articolo sono aumentate se il fatto di chi addestra o istruisce è commesso attraverso strumenti informatici o telematici». La norma con l'uso della congiunzione disgiuntiva "o" parrebbe infatti espressamente differenziare le due condotte.

[66] Cfr. D. FALCINELLI, *op. cit.* in nota 64, 85; M. LECCESE, *Il codice penale si allinea a Bruxelles. Ora chi predica l'odio rischia grosso. Punite anche le attività di arruolamento e addestramento*, in D&G, 2005, 95; A. PECCIOLI, *op. cit.* in nota 20, 773; M. PELISSERO, *op. cit.* in nota 18, 201; C. PIEMONTESE, *op. cit*. in nota 56, 1553; L. PISTORELLI, *op. cit.* in nota 18, 54; F. ROBERTI, *op. cit.* in nota 2, 531 s.; G. SALVINI, *op. cit.* in nota 18, 3375. Con riferimento alla condotta di addestramento e istruzione nel reato di cui all'art. 2-*bis* l. 895/1967, L. SCOTTO, *op. cit.* in nota 54, 493. Per una rico-

Con riferimento alla ripetitività del rapporto si è affermato che l'addestramento rappresenterebbe un reato abituale, mentre l'istruzione configurerebbe un reato unisussistente, potendosi integrare con una sola condotta[67]. Quanto ci sentiamo di escludere è che il maggior disvalore della condotta di addestramento – e che si pone a fondamento della pari punibilità del soggetto addestrato – possa ricercarsi nella mera individuazione del soggetto destinatario; non è, infatti, la determinatezza/indeterminatezza del destinatario dell'informazione ad assumere di per sé rilievo, quanto la creazione di un rapporto intersoggettivo fra maestro e recluta, del quale la prima rappresenta un mero presupposto[68].

La stessa Corte di Cassazione ha ritenuto di aderire all'opinione che ravvisa

> l'addestramento come contrassegnato da una vera e propria interazione tra l'addestratore e l'addestrato, che presupporrebbe (almeno di norma) un contatto diretto tra il primo ed il secondo, secondo i caratteri tipici dell'attività militare o paramilitare; addestrare è, dunque, rendere abile alle attività oggetto dell'addestramento, così da rendere punibile, allorché l'addestramento si sia compiuto e la "recluta" sia divenuta un vero e proprio "addestrato", anche quest'ultimo (art. 270 *quinquies*, ultimo periodo). […] Pare corretta la tesi di quella dottrina che ravvisa nel

struzione sintetica delle varie posizioni si veda: C. PAVARANI, *Addestramento ad attività con finalità di terrorismo anche internazionale*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Trattato di diritto penale. Parte speciale. Vol. I. I delitti contro la personalità dello Stato*, Milano, 2008, 410 ss.; V. REY, *Modifiche all'art. 270*-quinquies *c.p.*, in A. CONZ, L. LEVITA, *op. cit.* in nota 51, 20 s.; A. VALSECCHI, *Art. 270-quinquies c.p.*, in E. DOLCINI, G. MARINUCCI, *Codice penale commentato*, 4ª ed., Milano, 2015, 3025.

[67] S. COLAIOCCO, *Prime osservazioni…*, cit. in nota 51, 6. Nel suo complesso si tratterebbe dunque ad avviso di M. PELISSERO, *op. cit.* in nota 18, 201, di un reato eventualmente abituale.

[68] In tal senso riteniamo si debba leggere anche la precisazione di D. FALCINELLI, *op. cit.* in nota 64, laddove si afferma: «ovvio, peraltro, che non appena si individui "il" destinatario che tali informazioni faccia proprie, non appena si personalizzi dunque l'interrelazione, egli assumerà le vesti di addestrato in quanto posto all'altro capo di un definito e per questo concretamente penetrante rapporto di insegnamento di tecniche già in astratto tese (leggi, idonee) a formare o perfezionare (nell'aspetto teorico e pratico) una certa capacità "professionale", e dunque volte all'apprendimento delle modalità di svolgimento di una determinata funzione o di tenuta di un particolare comportamento».

> "fornire istruzioni" (anche) una diffusione *ad incertam personam*, che può essere effettuata pure a distanza, attraverso mezzi telematici e, quindi, nei confronti di soggetti che non si è in grado di stabilire se siano in grado di apprendere realmente le istruzioni impartite[69].

La precisazione della Suprema Corte secondo cui addestrare significherebbe rendere taluno abile all'oggetto di addestramento, impone di interrogarsi sul momento consumativo del reato in oggetto; tanto più alla luce dell'orientamento maggioritario che porta ad escludere la punibilità del tentativo, trattandosi di atti meramente preparatori[70].

---

[69] Cass. pen., Sez. VI, 20 luglio 2011 (dep. 25 luglio 2011), n. 29670, Pres. e Rel. De Roberto, in *Riv. pen.*, 2012, 56 ss.; in *Riv. pen.*, 2012, 1002 ss. (s.m.), con nota di F. PICCICHÈ, *Prime riflessioni della Corte di Cassazione sulla struttura del delitto di addestramento ad attività con finalità di terrorismo anche internazionale*, e in *Cass. pen.*, 2012, 897 ss., con nota di A. VALSECCHI, *L'accertamento del (doppio) dolo specifico nel reato di addestramento ad attività con finalità di terrorismo*; in *Dir. pen. cont.*, 20.12.2011, con nota di ID., *"Addestramento ad attività con finalità di terrorismo anche internazionale" (art. 270 quinquies c.p.): la prima pronuncia della Cassazione*; si veda anche F. PICCICHÈ, *Il problema del dolo nel reato di addestramento ad attività con finalità di terrorismo anche internazionale: due sentenze a confronto*, in *Dir. pen. cont.*, 19.09.2012.

[70] Cfr. C. PAVARANI, *op. cit.* in nota 66, 417; C. PIEMONTESE, *op. cit*. in nota 56, 1554; A. VALSECCHI, *Art. 270-quinquies c.p.*, cit. in nota 66, 3026. Si veda, tuttavia, Cass. pen. sez. I, 09 settembre 2015 (dep. 9 ottobre 2015), n. 40699, Rel. Sandrini, 50, in *Riv. pen.*, 2016, 50 ss., che con riferimento alla fattispecie di cui all'art. 270-*quater* c.p. (Arruolamento con finalità di terrorismo anche internazionale) ha affermato: «non può, peraltro, escludersi in via generalizzante e dogmatica l'ipotesi del tentativo punibile in rapporto a condotte poste in essere dal soggetto proponente e tese, con i caratteri di cui all'art. 56 c.p., (ed in presenza dei descritti presupposti di contesto e finalistici) al raggiungimento del suddetto accordo. Non è infatti la particolare natura del reato (di pericolo) ad impedire – di per sé – l'applicazione della generale previsione estensiva di cui all'art. 56 c.p., quanto la struttura della singola fattispecie (il che rende non pertinenti i richiami esposti dal Tribunale ad arresti di questa corte relativi a reato del tutto diverso) e la possibilità o meno di identificare in concreto una "progressione della esposizione a pericolo" dei beni giuridici protetti, come ritenuto – pur nell'ovvio contrasto di opinioni – da autorevole dottrina». La lettura della Corte è stata oggetto di forte critica in seno alla dottrina: M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale*, in *Terrorismo internazionale. Politiche della sicurezza. Diritti fondamentali*, *Edizione speciale QG*, settembre 2016, 111, il quale parla di sconfinamento del limite di legittima interpretazione della norma penale; M. DONINI, *Lotta al terrorismo e ruolo*

Nell'ambito di talune esperienze straniere ci si era, infatti, chiesti se l'addestramento presupponesse o meno una componente di risultato, ossia se per potersi dire realizzata una condotta di addestramento fosse richiesto un dominio effettivo da parte dell'allievo della tecnica trasmessa. In Germania dottrina minoritaria aveva ritenuto di poter individuare la necessità di un siffatto requisito[71]. La dottrina austriaca, mutuando il prevalente orientamento tedesco, tende invece ad escludere ai fini della punibilità dell'addestrato la necessità che l'addestramento sortisca un risultato positivo[72]. La riflessione straniera evidenzia come nel caso di specie si tratti di un reato di mera condotta (*schlichtes Tätigkeitsdelikt*)[73] per il quale non si richiede la realizzazione di un determinato risultato, esaurendosi il disvalore del fatto nella condotta stessa. La diversa lettura della norma innanzi richiamata poggia essenzialmente su esigenze di salvaguardia del principio di offensività; non si possono, tuttavia, sottacere in un'ottica realistica le difficoltà probatorie e

*della giurisdizione. Dal codice delle indagini preliminari a quello postdibattimentale*, in *Terrorismo internazionale*…, cit. in questa nota, 136, che vede in tale lettura la dimostrazione del ritorno dal diritto del fatto al diritto penale d'autore. Si consideri che con riferimento alla condotta attiva dell'addestramento la convenzione di Varsavia sul terrorismo prevedeva peraltro all'art. 9 co. 2 che gli Stati introducessero la punibilità del tentativo compatibilmente con il loro ordinamento, mentre l'art. 4 co. 4 della decisione quadro del 13 giugno 2002 (2002/475/GAI), come modificato dalla decisione quadro del 28 novembre 2008 (2008/919/GAI), prevedeva una possibilità per gli Stati membri in tal senso; tale possibilità è stata trasformata in obbligo di incriminazione nella proposta di direttiva (art. 16 co. 3). Per quanto riguarda invece la condotta passiva l'incriminazione da parte degli Stati membri è facoltativa (rapporto esplicativo, 6, § 42; l'art. 16 co. 3 della proposta di direttiva, infatti, non menziona fra i reati per i quali deve essere reso punibile in tentativo l'art. 8, atto di ricevere un addestramento a fini terroristici).

[71] D. STERNBERG-LIEBEN, *§ 89a Vorbereitung einer schweren staatsgefährdenden Gewalttat*, in A. SCHÖNKE, H. SCHRÖDER, *Strafgesetzbuch Kommentar*, 29ª ed., 2014, Monaco, 1351; *contra* C. BECKER, J. STEINMETZ, *op. cit.* in nota 46, 946; T. FISCHER, *op. cit.* in nota 46, 843; N. GAZEAS, *op. cit.* in nota 46, 752; J. SCHÄFER, *op. cit.* in nota 46, 125; M.A. ZÖLLER, *op. cit.* in nota 46, 25.

[72] F. PLÖCHL, *op. cit.* in nota 46, 92.

[73] I. MITGUTSCH, M. BRANDSTETTER, *Neues aus dem Besonderen Teil des StGB*, in I. MITGUTSCH, W. WESSELY (a cura di), *Strafrecht. Besonderer Teil. Jahrbuch 2011*, Wien, 2011, 18; F. PLÖCHL, *op. cit.* in nota 46, 92.

quindi la praticabilità processuale di una soluzione che richieda l'accertamento di una componente di risultato[74].

La riflessione porta ad emersione la tensione tra esigenze di salvaguardia dei principi ispiratori di un diritto penale liberale e la necessità di predisporre adeguati strumenti reattivi a fronte di gravi fatti di reato. Come è stato rettamente osservato

> la strada imboccata dal legislatore non è priva di rischi, giacché la repressione di comportamenti sintomatici, se spinta all'eccesso, può portare a un'eccessiva anticipazione della soglia di rilevanza penale dagli esiti incerti per le libertà fondamentali[75].

## *5. La finalità di terrorismo come strumento atto a delimitare la fattispecie*

L'anticipazione spinta della punibilità a condotte meramente prodromiche ha indotto la giurisprudenza italiana ad elaborare un criterio atto a delimitare la fattispecie in ossequio al principio di offensività.

A tal fine si è valorizzato l'elemento soggettivo richiesto dalla fattispecie di cui all'art. 270-*quinquies* c.p., recuperando il doppio dolo specifico al fine di tipizzare il fatto di reato; doppio dolo specifico individuato nella volontà di compiere atti di violenza o sabotaggio di servizi pubblici essenziali e dalla finalità di terrorismo.

---

[74] Al di là delle situazioni di agevole prova (ad esempio nel caso della costruzione di una bomba funzionante), la dimostrazione che l'addestramento abbia sortito effetto positivo potrebbe divenire assai ardua laddove manchi una condotta materiale dell'addestrato alla quale legare il giudizio. Ancora vi sarebbe da chiedersi cosa accada laddove per inettitudine dell'allievo questi non sia stato in grado di apprendere la tecnica trasmessa, facendo ad esempio esplodere la bomba che andava costruendo; caso realmente successo in Germania, si trattava però di un «autodidatta», cfr. BGH 3 StR 243/13, dell'8 maggio 2014, reperibile sul sito *www.bundesgerichtshof.de*; per un approfondimento si veda W. MITSCH, *Vorbeugende Strafbarkeit zur Abwehr terroristischer Gewalttaten*, in *NJW*, 2015, 209 ss.; la nota a sentenza di A. SINN, U. MOELLER, in *ZJS*, 2015, 232 ss.; R. WENIN, *L'addestramento per finalità di terrorismo…*, cit. in nota 51.

[75] L. PISTORELLI, *op. cit.* in nota 18, 56.

Secondo la già richiamata pronuncia della Suprema Corte n. 26970/2011[76], tali scopi non sarebbero da intendersi solamente quale particolare finalità del soggetto agente, ma dovrebbero al contempo riverberarsi in una oggettiva idoneità della condotta concretamente posta in essere a cagionare l'offesa perseguita, contribuendo così a "tipizzare" il fatto oggettivo di reato:

> allo scopo perseguito deve corrispondere – proprio per l'eccesso del momento volitivo, qui per ben due volte chiamato in causa – l'oggettiva idoneità della condotta a realizzare l'evento costituente l'obbiettivo della condotta. Tanto da far ritenere che tale idoneità (pur nell'immanenza della sua esclusiva base finalistica) costituisce un requisito immancabile per l'individuazione della stessa tipicità della condotta.

Facendo proprio l'orientamento dottrinale che ritiene l'elemento finalistico del dolo specifico idoneo a tipizzare il fatto oggettivo di reato, la Corte giunge quindi a qualificare la fattispecie in termini di reato di pericolo concreto. A riguardo occorre, tuttavia, precisare come la richiamata conclusione non sia affatto pacifica in dottrina, anzi. Se pur parrebbe generalmente condivisa la significazione tipizzante ed «oggettiva» del fine, si è al contempo evidenziato come rappresenterebbe in realtà il frutto di un equivoco l'esigere un requisito di oggettiva idoneità o prossimità causale del mezzo rispetto alla verificazione in concreto del risultato finalistico[77]. In tal modo, infatti, oltrepassando i limiti er-

[76] Si veda nota 69.

[77] L. PICOTTI, *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali*, Milano, 1993, 511 ss. Si veda anche ID., *Zwischen 'spezifischem' Vorsatz und subjektiven Unrechtselementen. Ein Beitrag zur typisierten Zielsetzung im gesetzlichen Tatbestand*, Berlin, 2014; F. ANGIONI, *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983, 115 s.; N. MAZZACUVA, *Il disvalore di evento nell'illecito penale. L'illecito commissivo doloso e colposo*, Milano, 1983, 224, nota 60; M. DONINI, *Teoria del reato*, in *Dig. disc. pen.*, XIV, 4ª ed., Torino, 1999, 264, nota 206; A. PAGLIARO, *Il reato*, Milano, 2007, 222; *contra* G. FORNASARI, *Dolo, errore ed* aberratio ictus, in AA.VV., *Introduzione al sistema penale*, vol. II, Torino, 2001, 176 s.; G. MARINUCCI, E. DOLCINI, *Manuale di diritto penale. Parte generale*, 4ª ed., Milano, 2012, 418; A. VALENTI, *Principi di materialità e offensività*, in AA.VV., *Introduzione al sistema penale*, vol. I, 4ª ed., Torino, 2012, 382 s.; in maniera differenziata, distinguendo

meneutici consentiti si trasformerebbero i reati a dolo specifico in una sorta di reati di pericolo concreto[78]; il che, come visto, è proprio ciò che fa la Corte.

Ora senza potersi soffermare in tale sede sulle diverse categorie dogmatiche elaborate, in particolare in seno alla dottrina straniera, sia evidenziato solo come non a caso in altri ordinamenti, si pensi alla Germania o all'Austria, la fattispecie sia stata inquadrata in termini di reato di pericolo astratto.

Ad avviso della Suprema Corte, dunque, la consumazione anticipata nei reati a dolo specifico presupporrebbe, perché il fatto non si esaurisca entro una fattispecie in cui assume un rilievo esorbitante l'elemento della volontà di scopo, che sussistano atti che oggettivamente rendano la detta volontà idonea a realizzare lo scopo. In altre parole, l'addestramento deve essere oggettivamente idoneo a consentire la realizzazione di un atto terroristico:

> La necessità di una severa tipizzazione dei singoli momenti strumentali che definiscono la condotta impone, quindi, un'altrettanto severa diagnosi sulla possibilità che quelle condotte descritte nell'art. 270-*quinquies* possano effettivamente realizzarsi non secondo modelli puramente didascalici (pur – almeno di norma – indispensabili nella struttura della fattispecie) ma concretamente idonei, nella loro intrinseca consistenza (da valutare *ex ante*, ma sulla base di elementi di fatto: spaziali, temporali, personali, etc.), da divenire verificabili dal giudice di merito nella loro proiezione verso il risultato rappresentato e voluto. Concludendo l'esame di tale aspetto strutturale della condotta descritta dall'art. 270-*quinquies*, può, dunque, inferirsene che se, per un verso, è il fine il momento di designazione del contegno che potrebbe altrimenti essere non punibile, per un altro verso, è l'idoneità dei mezzi che fa assumere rilevanza penale al fine, non essendo, in caso contrario, ipotizzabile alcuna offesa.

Come si vedrà meglio nel prosieguo, in tal modo la Cassazione recupera indirettamente l'elemento della volontà dell'addestrato a livello di tipicità, vincolando la punibilità dell'addestramento ad una concreta messa in opera del piano criminoso da parte dell'addestrato, così subor-

---

a seconda della tipologia di reato: F. MANTOVANI, *Diritto penale. Parte generale*, 8ª ed., Padova, 2013, 221.

[78] F. ANGIONI, *op. cit.* in nota 77, 115 s.

dinando implicitamente la punibilità dell'addestratore all'esistenza della volontà dell'addestrato a porre in essere una condotta terroristica, senza tuttavia richiedersi esplicitamente una consapevolezza della stessa in capo al primo, come invece espressamente statuito in altri ordinamenti[79] e dalla normativa sovranazionale.

Va rilevato che quella dottrina cui parrebbe richiamarsi la Corte è la stessa che nell'accertamento del pericolo nei reati di pericolo concreto richiede una prognosi *ex ante* in concreto a base totale[80]. E non pare essere un caso che nella sentenza menzionata la Corte di Cassazione arrivi a censurare la sentenza di merito sul presupposto, tra l'altro, che essa avesse omesso di argomentare – anzi implicitamente negato – che il ricorrente si stesse accingendo a mettere in pratica le nozioni che andava apprendendo. Il che però presupporrebbe la necessità/possibilità di individuare il destinatario passivo della condotta e ciò confligge, sotto il profilo della praticabilità, con la ricostruzione del fornire istruzioni in termini di condotta diffusiva *ad incertam personam*.

In senso critico si è, infatti, osservato:

> se la condotta di "fornire istruzioni" è integrata anche da una diffusione *ad incertam personam* – secondo quanto statuito in questa stessa sentenza dal Collegio – allora non si può al contempo esigere che il giudice del merito accerti la capacità del soggetto che ha ricevuto quelle istruzioni di tradurle in concrete azioni violente, perché ciò implicherebbe

[79] La norma austriaca, § 278e co. 1 StGB, che ricalca quelle che sono le indicazioni sovranazionali, in particolare l'art. 7 della Convenzione del Consiglio d'Europa, prevede in capo all'addestratore il seguente elemento soggettivo: la trasmissione del sapere, il fine terroristico, la consapevolezza che le tecniche trasmesse sono destinate ad essere utilizzate per tale fine. La norma richiede dunque che l'addestratore agisca con lo scopo di rendere l'addestrato abile alla commissione di una condotta terroristica nella consapevolezza della volontà dell'allievo di utilizzare quanto appreso per l'effettiva realizzazione di un reato terroristico. La condotta si incentra su di un elemento intellettivo, dato dalla consapevolezza della volontà dell'allievo di utilizzare quanto appreso per fini terroristici, e da un elemento volitivo, dato dal fine di rendere l'allievo abile per la commissione di un reato di terrorismo (ossia un addestramento con finalità di terrorismo), che costituisce il fine particolare in cui si sostanzia il dolo specifico secondo la concezione tradizionale accolta nella dogmatica italiana.

[80] G. MARINUCCI, E. DOLCINI, *Manuale di diritto penale. Parte generale*, 5ª ed. aggiornata da E. DOLCINI, G.L. GATTA, Milano, 2015, 226.

> quantomeno la necessità di identificare ogni volta i destinatari delle istruzioni e quindi di escludere la sussumibilità nella norma della condotta di diffusione di istruzioni *ad incertam personam*[81].

Ad avviso dell'autore da ultimo citato, il requisito dell'idoneità della condotta alla realizzazione dei fini oggetto del duplice dolo specifico, non andrebbe pertanto riferito alla capacità o alla disponibilità di mezzi per passare all'azione di chi quelle istruzioni ha ricevuto, quanto piuttosto alla effettiva utilità di quelle istruzioni a rendere edotto chiunque ne venga a conoscenza dei modi in cui si può usare un'arma, preparare una bomba, sabotare un servizio pubblico essenziale.

Sussistono tuttavia ragioni di natura sistematica che si frappongono ad una lettura che vincoli la *ratio* incriminatrice e l'elevato carico sanzionatorio della fattispecie in commento (reclusione da cinque a dieci anni) alla mera utilità oggettiva dell'informazione a rendere edotto il destinatario nell'uso dell'arma, ecc., e dunque all'informazione in sé considerata. Come si ricordava innanzi, l'art. 2-*bis* l. 895 del 1967 sanziona l'addestramento o la diffusione di istruzioni sull'uso di materiali esplosivi, di armi da guerra, di aggressivi chimici o di sostanze batteriologiche nocive o pericolose e di altri congegni micidiali con la reclusione da uno a sei anni. Si tratta di istruzioni relative a strumenti che possiedono un oggettivo maggiore potenziale offensivo rispetto a quelli di cui all'art. 270-*quinquies* c.p.

Se il criterio è quello della pericolosità oggettiva, motivo per il quale l'art. 2-*bis* sanziona la sola diffusione di istruzioni relative alle armi da guerra e non a quelle comuni e tale condotta viceversa è punita solo ove vi sia un fine di terrorismo, allora, affinché quanto punito non sia una mera intenzione, si richiede un dato oggettivo al quale ancorare la punibilità e addirittura la più severa cornice edittale.

Questo dato oggettivo potrà risiedere nel concreto pericolo per il bene giuridico che dovrà necessariamente passare attraverso la volontà dell'istruito di applicare quanto appreso per fini terroristici; appare, in-

[81] A. VALSECCHI, *"Addestramento ad attività con finalità di terrorismo anche internazionale"...*, cit. in nota 69. Si veda anche ID., *L'accertamento del (doppio) dolo specifico…*, cit. in nota 69, 911.

fatti, difficile rinvenire una connotazione terroristica nell'essenza dell'informazione stessa[82].

Le ragioni che spingono la Corte a ricercare un parametro oggettivo cui ancorare il disvalore del fatto, slegandolo dalla mera proiezione finalistica in senso soggettivo, sono di tutta evidenza, soprattutto in un settore, quello del terrorismo, in cui il rischio di una soggettivizzazione è assai elevato[83].

A fronte dell'inidoneità selettiva della fattispecie oggettiva, che finisce per ricomprendere condotte socialmente neutre, pare emergere il rischio che la norma possa diventare un «mero strumento di legittimazione legalistica di una scelta repressiva concreta»[84], magari fondata su valutazioni del tipo di autore.

Riemerge però a questo punto il problema dell'individuazione dei destinatari nel caso della diffusione *ad incertam personam*.

È qui che si evidenzia un secondo profilo di profonda criticità nella scelta legislativa italiana: il sanzionare nell'ambito di un'unica disposizione quattro condotte differenti: l'addestramento attivo, quello passi-

[82] Ma forse non necessariamente impossibile: si pensi all'ipotesi di istruzioni sulla realizzazione di un sabotaggio. Anche in tal caso, però, se è pur vero che si tratta di istruzioni che possiedono di per sé un carattere non socialmente neutro, al contempo, tuttavia, non hanno nemmeno connotazione strettamente terroristica.

[83] Con riferimento al terrorismo il diritto penale pare essere divenuto, secondo quanto evidenziato dalla più attenta dottrina, esso stesso uno strumento di lotta, se non di guerra: M. DONINI, *Lo* status *di terrorista*…, cit. in nota 63, 89; ID., *Il diritto penale di fronte al "nemico"*, in AA.VV., *Scritti per Federico Stella*, vol. I, Napoli, 2007, 102 ss. Si veda anche L. FERRAJOLI, *Il "diritto penale del nemico": un'abdicazione della ragione*, in A. BERNARDI, B. PASTORE, A. PUGIOTTO (a cura di), *Legalità penale e crisi del diritto, oggi. Un percorso interdisciplinare*, Milano, 2008, 167 s. e P. MOROSINI, *Continuità e novità della giurisprudenza in tema di terrorismo*, in *Questione giustizia*, 2006, 691 s., il quale facendo riferimento al rischio di una «funzionalizzazione bellicosa della macchina giudiziaria», evidenzia come l'analisi del modello di legalità antiterrorismo imponga «una riflessione di fondo sulla impostazione culturale e sul ruolo della giurisdizione nel circuito democratico in epoche di emergenza criminale».

[84] L'espressione è di F. SGUBBI, *Uno studio sulla tutela penale del patrimonio. Libertà economica, difesa dei rapporti di proprietà e «reati contro il patrimonio»*, Milano, 1980, 239.

vo, l'istruzione attiva e quella passiva[85], senza peraltro tracciare alcuna distinzione tra le due macro-categorie: addestramento ed istruzione, ma limitandosi ad introdurre una discutibile equiparazione *quod poenam* per il soggetto addestrato e ora, a seguito della modifica del 2015, di fatto anche solo istruito.

## *6. Una norma, più fattispecie?*

Come già ricordato, il d.l. n. 7 del 18 febbraio 2015 ha esteso la punibilità alla

> persona che avendo acquisito, anche autonomamente, le istruzioni per il compimento degli atti di cui al primo periodo, pone in essere comportamenti finalizzati alla commissione delle condotte di cui all'articolo 270-*sexies*.

La *ratio* dell'innovazione sarebbe da ricercarsi nella volontà di estendere la punibilità «anche ai terroristi che operano sganciati da sodalizi e da organizzazioni (cosiddetto lupo solitario)»[86].

La modifica normativa, lungi dal fugare i dubbi interpretativi, non riesce tuttavia a tracciare chiare linee di confine tra le varie condotte sanzionate e ad individuare i requisiti che dovrebbero contraddistinguere le stesse[87].

In particolare, la riforma, nel perseguire lo scopo espresso di sanzionare anche l'«auto-addestramento» – sul presupposto che la disposizione al tempo vigente richiedesse necessariamente l'esistenza di un rapporto duale tra addestratore e addestrato[88] –, estende la punibilità prevista per la persona addestrata alla

---

[85] Salve le precisazioni che seguiranno relativamente alla portata effettiva della novella del 2015.

[86] Disegno di legge di conversione (C. 2893), 6.

[87] Cfr. R. WENIN, *L'addestramento per finalità di terrorismo…*, cit. in nota 51, 12 ss.

[88] Cfr. la relazione accompagnatoria del disegno di legge di conversione (C. 2893), 6, laddove si dice che in ragione del fatto che la fattispecie «postula oggi un rapporto necessariamente duale tra addestratore e addestrato […] viene innestata una nuova fatti-

> persona che avendo acquisito, anche autonomamente, le istruzioni per il compimento degli atti di cui al primo periodo, pone in essere comportamenti univocamente finalizzati alla commissione delle condotte di cui all'articolo 270-sexies.

Laddove ci si arresti al mero dato normativo è difficile discostarsi dall'impressione che in realtà si sia infine introdotta una fattispecie nuova che non è quella dell'auto-addestramento, ma del reperimento di istruzioni per fini terroristici[89]. Ciò ha spinto parte della dottrina a ritenere attualmente configurabili nell'ordinamento italiano tre diverse condotte penalmente rilevanti: l'«etero-addestramento», l'«auto-addestramento» (già punibile in ragione della richiamata interpretazione estensiva del termine addestrare adottata dalla giurisprudenza)[90] e il reperimento di istruzioni per finalità di terrorismo (punibile in virtù della modifica normativa) solo a condizione che ad esso faccia seguito il compimento di atti univocamente finalizzati alla commissione di atti di terrorismo[91].

La conclusione sarà invece diversa laddove ci si muova in stretta aderenza alle finalità dichiarate dal legislatore, dando prevalenza ad un'interpretazione storica. In prima approssimazione, si dovrebbe ritenere innanzitutto non punibile l'«auto-addestramento» sotto la vigenza della previgente disciplina, con rigetto implicito della lettura offerta dalla giurisprudenza[92]. In secondo luogo ci si dovrebbe chiedere se la norma introduca una «nuova» condotta incriminata, quella del reperi-

---

specie di reato che rende punibile anche l'auto-addestramento, cioè la condotta di chi si prepara al compimento di atti di terrorismo, attraverso una ricerca e un apprendimento individuali e autonomi delle "tecniche" necessarie a perpetrare simili atti». Peraltro la giurisprudenza era già espressamente intervenuta interpretando la previsione normativa che estende la punibilità all'addestrato come comprendente oltre alla condotta di "etero-addestramento" anche quella di "auto-addestramento", ossia del soggetto che si "auto-addestri", Cass. pen., sez. I, 6 novembre 2013 (dep. 30 gennaio 2014), n. 4433, Pres. Giordano, Rel. Rombolà, in *Cass. pen.*, 2014, 4128 ss.

[89] Ipotesi assimilabile semmai alle fattispecie previste dal § 278f StGB austriaco e § 91 StGB tedesco.

[90] Cfr. nota 88.

[91] S. COLAIOCCO, *Prime osservazioni…*, cit. in nota 51, 8.

[92] Si tratterebbe in tale caso di fatto di una "interpretazione autentica" dell'art. 270-*quinquies* c.p.

mento di istruzioni, o si tratti di una tecnica descrittiva volta a disciplinare l'«auto-addestramento». A questo punto, ove si ritenga che, contrariamente alle finalità espresse nella relazione di conversione, si sia finito per introdurre una fattispecie diversa, ne consegue che l'unica forma di addestramento rilevante sarà quella dell'«etero-addestramento», fondata su di una relazione intersoggettiva. Va tuttavia evidenziato che l'auto-addestramento, pur non espressamente menzionato nel testo normativo, sarà punibile[93] per ragioni, oltre che di interpretazione storica, di "logica". Il reperimento di istruzioni, infatti, si pone in maniera necessariamente propedeutica rispetto all'addestramento in quanto tale, motivo per cui punendosi un *minus*/elemento imprescindibile dell'auto-addestramento si finirà di fatto per punire anche questo, salvo richiedersi un requisito ulteriore dato dal compimento di atti univocamente diretti alla realizzazione di condotte con finalità di terrorismo (elemento non richiesto nell'etero-addestramento).

Ciò precisato, nel dibattito austriaco ci si è chiesti se l'etero-addestramento penalmente rilevante richieda l'esistenza di un "rapporto collusivo" tra maestro e allievo, nel senso che il primo deve essere quantomeno a conoscenza delle intenzioni del secondo per potersi giustificare la punibilità di quest'ultimo[94]. Secondo un primo orientamento dovrebbe escludersi la necessità di un tale rapporto qualificato; non vi sarebbe, infatti, alcun elemento testuale che supporti una siffatta lettura ed anzi la norma mirerebbe a comprendere anche quelle situazioni nelle quali il terzo acquisisca con l'inganno l'addestramento necessario per perseguire le sue finalità illecite[95] e l'addestratore versi, dunque, in

[93] Cf. V. REY, *op. cit.* in nota 66, 24 s.; A. VALSECCHI, *Le modifiche alle norme incriminatrici in materia di terrorismo*, in R.E. KOSTORIS, F. VIGANÒ (a cura di), *op. cit.* in nota 14, 11; M. CAPUTO, *op. cit.* in nota 51, 93 s., quest'ultimo ritiene peraltro che per il rispetto del principio di uguaglianza il nuovo inciso debba valere anche per l'etero-addestrato; C.D. LEOTTA, *op. cit.* in nota 51, 17 ss.

[94] Per la punibilità dell'addestratore la fattispecie austriaca, al pari delle norme sovranazionali, richiede la conoscenza in capo allo stesso delle intenzioni terroristiche dell'allievo.

[95] F. PLÖCHL, *op. cit.* in nota 46, 92. Si tratta, anche in tal caso, di una posizione mutuata dalla dottrina tedesca: C. BECKER, J. STEINMETZ, *op. cit.* in nota 46, 946; T. FISCHER, *op. cit.* in nota 46, 843; J. SCHÄFER, *op. cit.* in nota 46, 125; D. STERNBERG-LIEBEN, *op. cit.* in nota 46, 1351.

buona fede. L'opposto orientamento[96], pur dando atto che la norma non richiede formalmente una «reciprocità di intenti», fa leva sull'esigenza di recuperare un livello minimo di pericolosità, tale da salvaguardare il principio di offensività. Lo sforzo interpretativo si regge sulla necessità di rinvenire una giustificazione all'irrogazione della pena che si ponga in coerenza con i principi fondamentali che dovrebbero permeare gli ordinamenti di ispirazione liberaldemocratica. A fronte di condotte socialmente adeguate[97], che si concretizzano nella trasmissione del sapere, lo sforzo va nella direzione di recuperare sul piano della tipicità un elemento selettivo di offensività rispetto ad una fattispecie nella quale rischia di assumere un ruolo esorbitante l'elemento volontaristico rappresentato dalla finalità perseguita dall'addestrato. L'esistenza di un rapporto collusivo e dunque di una comune direzione finalistica riuscirebbe a colmare, almeno in parte, quello che si definisce un disvalore del fatto annacquato nell'ambito di quanto si presenta dogmaticamente come un eccesso nell'anticipazione della soglia di rilevanza penale (*verwässerter Unrechtsgehalt eines verbrechensdogmatischen Vorverlagerungs-Exesses*)[98].

Con riferimento alla norma italiana la necessità di un siffatto requisito ricavato in via interpretativa potrebbe trovare conferma nella richiesta di un elemento ulteriore, il compimento di atti univocamente diretti, richiesto con riferimento al reperimento di istruzioni (e autoaddestramento), che dovrebbe colmare proprio l'assenza di quel rapporto intersoggettivo espressivo di una maggiore pericolosità[99]. Appare allora evidente che tale maggiore pericolosità che dovrebbe derivarsi dall'esistenza di un rapporto intersoggettivo non potrà fondarsi sull'esistenza del rapporto in quanto tale, ma sulle caratteristiche che esso deve

[96] N. GAZEAS, *op. cit.* in nota 46, 753; N. GAZEAS, T. GROSSE-WILDE, A. KIEßLING, *Die neuen Tatbestände im Staatsschutzstrafrecht. Versuch einer ersten Auslegung der §§ 89a, 89b und 91 StGB*, in *NStZ*, 2009, 597 s.; H.-U. PAEFFGEN, *op. cit.* in nota 46, 218; M.A. ZÖLLER, *op. cit.* in nota 46, 25.

[97] Il richiamo è al canone welzeliano dell'adeguatezza sociale delle singole condotte.

[98] H.-U. PAEFFGEN, *op. cit.* in nota 46, 218.

[99] Sul punto ci si era già soffermati in R. WENIN, *L'addestramento per finalità di terrorismo…*, cit. in nota 51, 17 s.

possedere nell'essere espressione di un maggiore disvalore del fatto e che dunque risiede nell'esistenza della richiamata relazione collusiva rispetto al compimento di atti di terrorismo. Diversamente opinando sarebbe difficile riuscire a spiegare in cosa consista la maggiore pericolosità del soggetto che invece di limitarsi a leggere un libro di chimica segua un corso universitario dedicato al tema durante il quale il sapere gli viene trasmesso da terzi. Una lettura questa che permetterebbe anche di superare l'obiezione di una possibile violazione del principio di uguaglianza senza dover estendere il nuovo requisito del compimento di atti univocamente diretti alla realizzazione di condotte con finalità di terrorismo all'etero-addestramento[100].

### *6.1. La soluzione adottata dagli ordinamenti stranieri*

Molti ordinamenti stranieri di *civil law* disciplinano addestramento e istruzione nell'ambito di due norme distinte[101], prevedendo altresì una cornice edittale differenziata in ragione del diverso disvalore del fatto[102].

Accanto alla maggior determinatezza nella descrizione delle fattispecie, ciò consentirebbe di superare le obiezioni circa l'incompatibilità con la diffusione *ad incertam personam* della consapevolezza in capo al

[100] Cfr. quanto riportato in nota 93 con riferimento alla posizione di Caputo.

[101] Es. in Austria si tratta rispettivamente dei § 278e StGB Addestramento per finalità terroristiche (*Ausbildung für terroristische Zwecke*) e § 278f StGB Istruzione per il compimento di una condotta terroristica (*Anleitung zur Begehung einer terroristischen Straftat*); in Germania del § 89a StGB Preparazione di una grave condotta violenta tale da mettere in pericolo lo Stato (*Vorbereitung einer schweren staatsgefährdenden Gewalttat*) e § 91 StGB Istruzione per il compimento di una grave condotta violenta tale da mettere in pericolo lo Stato (*Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat*).

[102] Esiste, infatti, un'evidente differenza a livello di offensività fra le varie condotte che, secondo schemi purtroppo ormai consolidati, non è stata valorizzata in sede di tipizzazione legislativa con conseguente rimessione alla discrezionalità giudiziaria. Cfr. M. CAPUTO, *op. cit.* in nota 51, 97 s. Ad avviso di M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione*, cit. in nota 70, 139, l'equiparazione sanzionatoria, frutto del livellamento punitivo di associato, addestratore, addestrato e auto-addestrato esterno indipendente, evidenzierebbe la rottura del valore tipizzante del vincolo associativo, come già avvenuto nell'ambito della lotta alla mafia.

maestro del fine terroristico che muove l'allievo e che è richiesta espressamente dalle norme sovranazionali.

### *6.2.1. La consapevolezza dell'addestratore circa la finalità terroristica in capo all'allievo*

La punibilità dell'addestratore richiede nelle esperienze straniere, in conformità alle norme sovranazionali, la consapevolezza sull'utilizzo che sarà fatto dell'addestramento impartito, così ad esempio: Regno Unito (Art. 6 *Terrorism Act 2006*), Austria (§ 278e StGB)[103], Germania (§ 89a StGB), Stati Uniti (§ 2339A *U.S. Code Title 18 – Crimes and criminal Procedure*).

Tale consapevolezza rappresenta il disvalore del fatto rispetto a condotte, in ipotesi, socialmente neutre.

Peraltro non si può certamente sottacere, come evidenziato ad esempio dalla dottrina austriaca[104], il problema relativo alla «praticabilità processuale» della fattispecie a livello di probatorio, laddove ai fini della punibilità dell'addestratore sia richiesta la prova che questi abbia agito con finalità di terrorismo, essendo a conoscenza delle intenzioni terroristiche dell'allievo. In particolare tale secondo elemento richiede l'accertamento di un doppio elemento soggettivo che si articola, secondo un criterio di ordine logico, *in primis* nell'accertamento di un'effettiva volontà dell'allievo di utilizzare quanto appreso per un fine terroristico e quindi della conoscenza di tale volontà in capo all'addestratore.

[103] Va rilevato che la norma austriaca rispetto alle norme sovranazionali è formulata in maniera più precisa: mentre, infatti, le norme internazionali richiedono la consapevolezza che le istruzioni impartite sono intese per conseguire tale obiettivo, il che potrebbe dare adito a dubbi interpretativi circa fatto che la volontà di impiego debba sussistere anche in capo al destinatario delle informazioni, il § 278e StGB richiede espressamente la consapevolezza in capo all'addestratore che le informazioni saranno impiegate per i fini indicati («wenn er weiß, dass die vermittelten Fähigkeiten für diesen Zweck eingesetzt werden sollen») e quindi, come visto, la volontà dell'addestrato di impiegare le informazioni per i fini richiamati cfr. F. PLÖCHL, *op. cit.* in nota 46, 93

[104] Cfr. H. HINTERHOFER, C. ROSBAUD, *Strafrecht. Besonderer Teil II. §§ 169-321 StGB*, 5ª ed., 2012, Wien, 320. Sul punto si veda, tuttavia, la precisazione di cui in nota 103 che potrebbe differenziare il portato della norma austriaca da quello dell'altre disposizioni, in particolare da quelle sovranazionali.

Non è necessario, è vero, che si realizzi una condotta terroristica, ma al contempo le norme richiedono che tale volontà esista e sia conosciuta al momento dell'atto di addestramento, rappresentando un elemento imprescindibile per la punibilità dell'addestratore nel quale si incentra il disvalore del fatto. Detto in altre parole, laddove l'addestratore agisse con il fine di rendere abile l'allievo alla commissione di un atto terroristico, ma mancasse in quest'ultimo la volontà di applicare quanto appreso per tale fine o una siffatta volontà non fosse conosciuta dall'addestratore se ne dovrebbe escludere la punibilità.

La consapevolezza in capo all'addestratore dell'utilizzo che sarà fatto delle abilità trasmesse rappresenta in ogni caso un elemento imprescindibile al fine di selezionare le condotte realmente meritevoli di sanzione; certamente ci si potrebbe poi interrogare circa l'intensità di tale l'elemento soggettivo, differenziando poi la relativa sanzione. Così ad esempio il codice penale federale australiano estende la punibilità anche al soggetto che addestri taluno agendo con *recklessness*[105] rispetto alla "connessione terroristica"[106].

---

[105] Cfr. Criminal Code Act 1995 5.4. Recklessness.

(1) A person is reckless with respect to a circumstance if: (a) he or she is aware of a substantial risk that the circumstance exists or will exist; and (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

(2) A person is reckless with respect to a result if: (a) he or she is aware of a substantial risk that the result will occur; and (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

(3) The question whether taking a risk is unjustifiable is one of fact.

(4) If recklessness is a fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element.

Sulla *recklessness* nel sistema penale australiano cfr. J. GANS, *Modern Criminal Law of Australia*, Melbourne, 2012; S. ODGERS, *Principles of Federal Criminal Law*, 3ª ed., Sidney, 2015. Per un'analisi dell'istituto nell'ambito del sistema inglese cfr. F. CURI, Tertium datur. *Dal* common law *al* civil law *per una scomposizione tripartita dell'elemento soggettivo del reato*, Milano, 2003, 47 ss.; G.P. DEMURO, *Il dolo. Vol. II. L'accertamento*, Milano, 2010, 221 ss.; S. VINCIGUERRA, *Introduzione allo studio del diritto penale inglese. I principi*, Padova, 1992, 187 ss. Per un inquadramento generale nell'ambito dei Paesi di *common law*: A. CADOPPI, voce *Mens rea*, in *Dig. disc. pen.*, vol. VII, 4ª ed., Torino, 1993, 618 ss.

[106] Criminal Code Act 1995. 101.2 Providing or receiving training connected with terrorist acts.

Con riferimento all'esperienza italiana la necessaria consapevolezza del fine terroristico si potrebbe peraltro ricavare in via interpretativa proprio sulla base del supporto argomentativo offerto dalla norma sovranazionale[107], in particolare dalla decisione quadro, e dalle norme straniere attuative della stessa, ma è evidente che un'espressa previsione normativa sarebbe stata in ogni caso preferibile e possibile solo laddove, per quanto detto, si fossero disciplinati in maniera autonoma addestramento e istruzione. Come già ricordato, in ogni caso la giurisprudenza italiana[108] recupera indirettamente l'elemento della volontà dell'addestrato a livello di tipicità, mutuandola dalla riflessione sul dolo specifico che deve caratterizzare le condotte di cui all'art. 270-*quinquies* c.p. e quindi da elementi concreti di idoneità espressivi di quella volontà riprovevole. Nel vincolare la punibilità dell'addestramento ad una concreta messa in opera del piano criminoso da parte dell'addestrato, la Corte di fatto subordina implicitamente la punibilità dell'addestratore

(1) A person commits an offence if: (a) the person provides or receives training; and (b) the training is connected with preparation for, the engagement of a person in, or assistance in a terrorist act; and (c) the person mentioned in paragraph (a) knows of the connection described in paragraph (b). Penalty: Imprisonment for 25 years.

(2) A person commits an offence if: (a) the person provides or receives training; and (b) the training is connected with preparation for, the engagement of a person in, or assistance in a terrorist act; and (c) the person mentioned in paragraph (a) is reckless as to the existence of the connection described in paragraph (b). Penalty: Imprisonment for 15 years.

[107] Sul possibile utilizzo ermeneutico in *bonam partem* delle decisioni quadro, con effetti limitativi dell'ambito di rilevanza penale in relazione alla normativa nazionale si veda: V. MANES, *L'incidenza delle «decisioni-quadro» sull'interpretazione in materia penale: profili di diritto sostanziale*, in *Cass. pen*., 2006, 1150 ss.; F. VIGANÒ, *Recenti sviluppi in tema di rapporti tra diritto comunitario e diritto penale*, in *Dir. pen. proc.*, 2005, 1438. In generale sul tema si veda: F. VIGANÒ, *Il giudice penale e l'interpretazione conforme alle norme sovranazionali*, in P. CORSO, E. ZANETTI (a cura di), *Studi in onore di Mario Pisani*, vol. II, Piacenza, 2010, 617 ss.; V. MANES, *Il giudice nel labirinto. Profili delle intersezioni tra diritto penale e fonti sovranazionali*, Roma, 2012, e i contributi in F. SGUBBI, V. MANES (a cura di), *L'interpretazione conforme al diritto comunitario in materia penale*, Bologna, 2007.

[108] Cass. pen., Sez. VI, 20 luglio 2011 (dep. 25 luglio 2011), n. 29670, Pres. e Rel. De Roberto, cit. in nota 69.

all'esistenza della volontà dell'addestrato a porre in essere una condotta terroristica.

### *6.2.2. La punizione della condotta del fornire istruzioni*

L'esperienza straniera offre un dato interessante di riflessione anche in materia di istruzione, offrendo un parametro oggettivo cui ancorare il disvalore del fatto e superare così l'*impasse* di cui si diceva in precedenza[109].

Sia in Austria, sia in Germania, si richiede, infatti, ai fini della punibilità dell'istruzione, accanto alla finalità terroristica, che le informazioni siano idonee alla realizzazione di un fatto di terrorismo e che la diffusione avvenga in modo tale da istigare al compimento dello stesso; si tratta, ossia, di una forma di istigazione indiretta, che si realizza mediante le particolari modalità di diffusione delle informazioni.

Non si può certo sottacere come la necessità di un accertamento concreto impegni il giudice in un compito tutt'altro che agevole, con il rischio che tale accertamento sull'idoneità della condotta ad istigare si risolva in concreto in un ampio margine di discrezionalità giudiziale che in quanto tale rischia di pregiudicare la necessaria prevedibilità ed uniformità di giudizi[110], tuttavia, tale elemento di pericolosità espressa si giustifica in ragione dello sforzo volto a ricercare una maggiore selettività a fronte di condotte potenzialmente neutre.

Se nel contesto italiano la richiesta idoneità[111] delle istruzioni rappresenta un rimedio volto ad impedire che assuma un ruolo esorbitante l'elemento della volontà di scopo, sotto il profilo probatorio si è al con-

[109] Ci si riferisce al problema relativo alla lettura del fornire istruzioni come diffusione *ad incertam personam* e al requisito di pericolosità individuato dalla Suprema Corte per ritenere integrata la fattispecie.

[110] Cfr. sul 414 c.p. italiano C. VISCONTI, *Art. 414. Istigazione a delinquere*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Trattato di diritto penale. Parte speciale. Vol. III. I delitti contro l'amministrazione della giustizia. I delitti contro il sentimento religioso e la pietà dei defunti. I delitti contro l'ordine pubblico*, Milano, 2008, 1043; G. FORNASARI, *Art. 414. Istigazione a delinquere*, in G. FORNASARI, S. RIONDATO (a cura di), *Reati contro l'ordine pubblico*, Torino, 2013, 1 ss.

[111] Si ricordino però i profili problematici che la lettura del dolo specifico avanzato dalla Suprema Corte con la sentenza n. 29670/2011 pone, cfr. nota 77.

tempo richiesto l'accertamento di un'effettiva direzione finalistica rispetto a istruzioni potenzialmente idonee all'utilizzo in attentati terroristici. In tal senso si è precisato che tale finalità dovrà essere resa evidente tramite proclami o appelli che manifestino come le istruzioni siano impartite per finalità terroristiche[112], dovendosi in caso contrario, come nelle ipotesi di pagine internet che informino sulla costruzione di ordigni esplosivi, ma non siano connotate da alcun proclama, tendenzialmente escludersi la configurabilità del reato di cui all'art. 270-*quinquies*[113]. Si finisce, dunque, per vincolare l'accertamento del fine terroristico a quegli stessi elementi elevati a criterio probatorio della "idoneità istigatoria" richiesta dalla fattispecie austriaca. La "pericolosità" dell'informazione va dunque ricercata non tanto, o meglio non solo nella sua natura, quanto nelle modalità di "trasmissione" e dunque nell'idoneità della condotta nella sua complessità a favorire la commissione di una condotta terroristica.

## *7. L'acquisizione di istruzioni per finalità terroristiche*

Anche in tal caso la modifica normativa ha dato adito ad ampio dibattito nello sforzo di ricostruire il reale contenuto della nuova fattispecie incriminatrice. Non è possibile per gli scopi del presente scritto soffermarsi su tutti gli aspetti problematici, ci si limiterà a proporre alcune riflessioni con particolare riferimento alle "nuove tecnologie".

Come ricordato, la modifica del 2015 ha esteso la sanzione alla

> persona che avendo acquisito, anche autonomamente, le istruzioni per il compimento degli atti di cui al primo periodo, pone in essere comportamenti univocamente finalizzati alla commissione delle condotte di cui all'articolo 270-sexies.

[112] Si tratta ossia di quegli elementi di contesto richiamati dallo stesso legislatore austriaco.

[113] C. PAVARANI, *op. cit.* in nota 66, 412.

### *7.1. La nozione dell'acquisire*

Il primo profilo problematico attiene alla scelta terminologica dell'acquisire, tenuto altresì conto del contesto primario al quale pare volersi riferire il legislatore, ossia quello informatico. Il termine acquisire rappresenta, infatti, pressoché un *novum* per il codice penale[114], differenziandosi in particolare dalla terminologia adottata con riferimento alla detenzione di materiale pedopornografico, laddove si fa riferimento alla condotta del procurarsi e detenere, come anche da quella degli artt. 256, 257 e 258 c.p. nei quali al pari si punisce il procurarsi notizie. La scelta del legislatore impone dunque di interrogarsi in primo luogo sul contenuto della condotta incriminata, se si tratti di un mero sinonimo del termine procurarsi o si sia consapevolmente inteso fare riferimento a qualcosa di diverso. La questione assume peraltro un rilievo più limitato rispetto ad altre realtà straniere. Nella struttura della fattispecie italiana l'acquisizione delle istruzioni non rappresenta, infatti, la condotta sottoposta a pena, ma un presupposto di questa, la quale viene integrata dalla realizzazione di comportamenti univocamente finalizzati alla commissione di atti di terrorismo[115]. In altre realtà quanto si punisce è invece già il semplice reperimento delle informazioni per finalità di terrorismo[116]. La scelta italiana porta ad evidenza la necessità di an-

[114] Il termine compare talune volte nel codice (es. artt. 322-*ter*, 335-*bis*, 377-*bis*, 416-*bis*, 727), ma è soprattutto l'uso terminologico ad essere assolutamente "innovativo".

[115] Come già si era evidenziato in R. WENIN, *L'addestramento per finalità di terrorismo…*, cit. in nota 51, 15. Si veda quanto precisato da D. FERRANTI, Presidente Commissione Giustizia, Resoconto della seduta del 18 marzo 2015 delle Commissioni Riunite (II e IV), 9; *Dossier* del Servizio Studi del Senato sull'A.S. n. 1854, aprile 2015 n. 204, 24 s., entrambi disponibili sul sito del Senato, *www.senato.it*. Nello stesso senso: M. CAPUTO, *op. cit.* in nota 51, 95 s.; S. COLAIOCCO, *Prime osservazioni…*, cit. in nota 51, 7 ss.; ID., *Le nuove norme antiterrorismo…*, cit. in nota 51, 3 s.; F. FASANI, *Le nuove fattispecie antiterrorismo…*, cit. in nota 51, 942; G. LEO, *op. cit*. in nota 51; G. MARINO, *op. cit.* in nota 51, 1412; A. PECCIOLI, *op. cit.* in nota 20, 773; V. REY, *op. cit.* in nota 66, 25; A. VALSECCHI, *Le modifiche alle norme…*, cit. in nota 93, 11 s., ID., *Art. 270-quinquies c.p.*, cit. in nota 66, 3025; A. VARVARESSOS, *Nuove misure di contrasto al terrorismo di matrice internazionale*, in AA.VV., *Commento al decreto legge 7/2015…*, cit. in nota 51, 13 s.

[116] Cfr. Austria, Germania, Regno Unito.

corare il giudizio di offensività del fatto ad un criterio che travalichi la mera proiezione finalistica, richiedendosi indi un elemento ulteriore espresso[117].

Rimane in ogni caso l'imbarazzo sull'attribuzione di significato, che si sarebbe potuto evitare ricorrendo ad una terminologia già consolidata.

Anche in tal caso il raffronto con esperienze straniere offre un interessante banco di prova. In Germania e in Austria si fa, infatti, riferimento alla condotta del procurarsi (*sich verschaffen*) che presupporrebbe una condotta finalizzata a procacciarsi la disponibilità[118]. Il legislatore austriaco si richiama alla fattispecie di cui al § 207a StGB in materia di pornografia minorile e all'interpretazione datane in dottrina e giurisprudenza. Con riguardo al § 207a, nel tracciare una distinzione tra le condotte del procurarsi e detenere[119] descritte al comma 3, si è affermato che il procurarsi richiederebbe un'autonoma iniziativa volta ad acquistare la disponibilità sul materiale vietato (scaricamento da internet, salvataggio su di un supporto informatico, stampa dell'immagine, ecc.)[120], mentre la detenzione presupporrebbe una qualsiasi disponibili-

[117] Elemento selettivo che la giurisprudenza (Cass. pen. 29670/2011, cit. in nota 69), nel silenzio normativo, aveva ritenuto di ricavare in via interpretativa richiamandosi alla significazione tipizzante ed «oggettiva» del fine del dolo specifico.

[118] *Terrorismuspräventionsgesetz* 2010, 674 BlgNr 24. GP, 6: «Die Tathandlung des Sich-Verschaffens aus dem Internet im Sinne des Abs. 2 setzt das Abspeichern auf einem Speichermedium voraus, da der Täter beim Sich-Verschaffen ein eigenes Zutun zur Gewahrsamserlangung setzen muss (vgl. Schick, WK-StGB2, § 207a, Rz 20)».

[119] Si tratta di una formulazione molto simile a quella dell'art. 600-*quater* c.p.

[120] Riprendendo la dottrina tedesca sul punto: W. AUER, B. LOIMER, *Zur Strafbarkeit der Verbreitung von Kinderpornographie über das Internet*, in *ÖJZ*, 1997, 618; C. BERTEL, K. SCHWAIGHOFER, *Österreichisches Strafrecht, Besonderer Teil. Teil II. (§§ 169 bis 321j StGB)*, Wien, 2015, 71; H. HINTERHOFER, *§ 207a Pornographische Darstellungen Minderjähriger*, 14. Lfg. (November 2006), in O. TRIFFTERER, H. HINTERHOFER, C. ROSBAUD (a cura di), *Salzburger Kommentar zum Strafgesetzbuch*, vol. 5, Wien, 16; T. PHILIPP, *§ 207a Pornographische Darstellungen Minderjähriger*, 108. Lfg. (März 2014), in F. HÖPFEL, E. RATZ (a cura di), *op. cit.* in nota 46, 67; OHG dell'11.02.1999, 15 Os 190/98, in *Juristische Blätter*, 2000, 534. Anche la Commissione di giustizia austriaca aveva mostrato di condividere tale ricostruzione allorquando la norma nel 1994 fu introdotta nell'ordinamento austriaco, cfr. JAB 1848 BlgNr 18. GP, 3. Tale lettura trova peraltro l'avallo non solo della dottrina, ma anche del legislatore

tà di fatto. La detenzione andrebbe dunque a ricomprendere tutte le ipotesi nelle quali il soggetto acquisisca la disponibilità non per effetto di una propria condotta o, ancora, in maniera involontaria (ricezione di una mail indesiderata, ecc.)[121]. È interessante notare come invece in Italia, a fronte della medesima formulazione, con riferimento alla fattispecie analoga dell'art. 600-*quater* c.p. sia stata avanzata la proposta di una lettura interpretativa fondata su ragioni sistematiche che vede il tratto differenziale nel diverso autore dell'oggetto della condotta, per cui per detenzione si intenderebbe l'acquisizione della disponibilità del materiale senza ottenerlo da altri, ossia attraverso la produzione dello

tedesco che nel disegno di legge volto a sanzionare la preparazione di gravi condotte violente tali da mettere in pericolo lo Stato (Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten) precisa, infatti, la necessità di una volontà volta a procurarsi il materiale che difetta nel caso della ricezione indesiderata di una comunicazione: «Ebenso ist ein bei dem Verschaffenden zumindest konkludent vorhandener Wille zur Begründung des Besitzes an der Schrift erforderlich, der etwa bei unverlangten E-Mail-Zusendungen nicht gegeben ist» (BT-Drucksache 16/12428, 18).

[121] Per escludersi la punibilità sarebbe necessaria un'eliminazione fisica o virtuale definitiva (non il semplice spostamento nel cestino) del documento di cui si sia entrati involontariamente in possesso: H. HINTERHOFER, *§ 207a…*, cit. in nota 120, 17; H. HINTERHOFER, C. ROSBAUD, *op. cit.* in nota 104, 148. In tal senso si è peraltro espressa anche la Cassazione italiana: Cass. pen., sez. III, 16 gennaio 2014 (dep. 5 marzo 2014), n. 10491, Pres. Teresi, Rel. Pezzella; Cass. pen., sez. III, Sent., 06 ottobre 2010 (dep. 13 gennaio 2011), n. 639, Pres. Squassoni, Rel. Amoroso, in *Cass. pen.*, 2012, 532 ss. con nota di L. GIZZI, *Integra il reato di cui all'art. 600*-quater *c.p. anche la semplice visione di materiale pedopornografico scaricato da* internet. Tesi fatta propria anche in Germania: cfr. T. HÖRNLE, *§ 184b Verbreitung, Erwerb und Besitz kinderpornographischer Schriften*, in W. JOECKS, K. MIEBACH (a cura di), *op. cit.* in nota 46, 1591. Nella dottrina italiana sul punto si veda A. CADOPPI, *Art. 600-quater. Detenzione di materiale pornografico*, in ID. (a cura di), *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, 4ª ed., Padova, 2006, 227 ss. e dottrina ivi citata, in particolare in nota 1; S. DELSIGNORE, *La detenzione di materiale pornografico minorile: un reato che poggia solamente sul biasimo morale e sul sospetto di condotte realmente offensive per la personalità dei minori?*, in M. BIANCHI, S. DELSIGNORE (a cura di), *I delitti di pedopornografia fra tutela della moralità pubblica e dello sviluppo psico-fisico dei minori*, Padova, 2008, 84 ss.; M. DONINI, *"Danno" e "offesa" nella c.d. tutela penale dei sentimenti*, in *Riv. it. dir. proc. pen.*, 2008, 1579 s.

stesso per uso personale[122]. Più aderente alla proposta interpretativa austriaca è la tesi che vede nel procurarsi un concetto dinamico comprendente una qualche attività diretta ad entrare nella disponibilità del materiale, mentre la detenzione atterrebbe alla compiuta acquisizione di fatto a qualsiasi titolo[123].

Al pari di quanto sostenuto in Italia[124], anche in Austria si ritiene che il mero "consumo" di materiale pedopornografico, ossia la semplice visualizzazione o consultazione di immagini in internet non integri la condotta tipica del procurarsi e detenere[125]. La soluzione tuttavia non è univoca nella dottrina e giurisprudenza di altri Paesi; così in Germania si è avuto modo di sostenere che già la semplice visualizzazione integrerebbe la fattispecie[126].

---

[122] F. MANTOVANI, *Diritto penale. Parte speciale*, vol. 1, 5ª ed., Padova, 2013, 516. La *ratio* dell'autonoma punizione del procurarsi sarebbe da ricercarsi nella possibilità di reprimere penalmente il tentativo di procurarsi il materiale, che non sarebbe punibile a livello di tentativo di detenzione: A. CADOPPI, *Art. 600-quater…*, cit. in nota 121, 231.

[123] E. MENGONI, *Delitti sessuali e pedofilia*, Milano, 2008, 287.

[124] A. CADOPPI, *Art. 600-quater…*, cit. in nota 121, 232 s.; P. CORDERO, *Considerazioni in tema di detenzione di materiale pedo-pornografico*, in *Dir. pen. proc.*, 2003, 1168; L. GIZZI, *op. cit.* in nota 121, 538; S. DELSIGNORE, *op. cit.* in nota 121, 100; P. PERRI, *Profili informatico-giuridici della diffusione, mediante strumenti telematici, di materiale pedopornografico*, in *Cass. pen.*, 2008, 3471, nota 17; L. PICOTTI, *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in AA.VV., *Scritti per Federico Stella*, vol. II, Napoli, 2007, 1314. In particolare con la modifica apportata nel 2006, che ha sostituito il termine «disporre» con quello del «detenere», il legislatore avrebbe escluso definitivamente interpretazioni volte a far ricadere nella fattispecie la mera consultazione; in tal senso G. COCCO, *Può costituire reato la detenzione di pornografia minorile?*, in *Riv. it. dir. proc. pen.*, 2006, 882 s.; S. DELSIGNORE, *op. cit.* in nota 121, 100.

[125] W. AUER, B. LOIMER, *op. cit.* in nota 120, 618; C. BERTEL, K. SCHWAIGHOFER, *op. cit.* in nota 120, 71; H. HINTERHOFER, *§ 207a…*, cit. in nota 120, 17; T. PHILIPP, *op. cit.* in nota 120, 67; JAB 1848 BlgNr 18. GP, 3; JAB 106 BlgNr 24. GP, 34.

[126] OLG Hamburg del 15.02.2010 - 2-27/09 (REV), in *Neue Juristische Wochenschrift*, 2010, 1893, con nota di L. MINTAS; OLG Schleswig del 15.09.2005 - 2 Ws 305/05, in *Neue Zeitschrift für Strafrecht - Rechtsprechungsreport*, 2007, 41 ss.; K. ECKSTEIN, *Grundlagen und aktuelle Probleme der Besitzdelikte – EDV, EU, Strafrechtsänderungsgesetze, Konkurrenzen*, in *Zeitschrift für die gesamte Strafrechtswissenschaft*, 2006, 120 s.; H.-W. MORITZ, *Strafbarkeit*, in U. LOEWENHEIM, F.A. KOCH (a cura di), *Praxis des Online-Rechts*, München, 2001, 525 s.; BT-Drucksache 18/2601,

Vi sarebbe poi da interrogarsi sul fatto se la navigazione *online* e il salvataggio automatico nella *cache* del *browser*[127] possano integrare la condotta dell'acquisire. A riguardo si è avuto modo di precisare che il salvataggio automatico nella *directory* temporanea dei *file* di internet fa sì che il materiale venga ad essere presente nel *computer* «anche senza che l'agente abbia compiuto atti idonei a tal fine ed entra nella materiale disponibilità del soggetto, che se lo è procurato nel momento stesso della navigazione»[128]. L'affermazione, tuttavia, per quanto diffusa an-

34. La riflessione talora sovrappone in realtà due diversi aspetti, quello della visualizzazione *online* e quello del salvataggio nella *cache* del *browser* dei file visionati: cfr. in tal senso: T. FISCHER, *§ 184b Verbreitung, Erwerb und Besitz kinderpornographischer Schriften*, in ID., *Strafgesetzbuch…*, cit. in nota 46, 1322. Si tratta tuttavia di due profili che dovrebbero essere tenuti separati, non essendo necessariamente congiunti, potendosi infatti anche disattivare il salvataggio automatico. Per un inquadramento generale in lingua italiana della disciplina tedesca in materia si veda: M. HELFER, *Sulla repressione della prostituzione e pornografia minorile. Una ricerca comparatistica*, Padova, 2007; M. L'INSALATA, *La disciplina normativa della pedo-pornografia in Germania*, in M. BIANCHI, S. DELSIGNORE (a cura di), *op. cit.* in nota 121, 181 ss. La circostanza che il legislatore tedesco nel recepire la Convenzione di Lanzarote abbia ritenuto opportuno sanzionare espressamente l'"accesso" a materiale pedopornografico mediante tecnologie dell'informazione e della comunicazione, si giustifica proprio in ragione del dibattito sul fatto se il mero "visualizzare" possa o meno ritenersi idoneo ad integrare gli estremi del procurarsi e del detenere, presupponendo quest'ultimi la disponibilità del materiale, la cui sussistenza potrebbe ritenersi dubbia nell'ipotesi della mera visualizzazione: «Unter Berücksichtigung der Rechtsprechung und der herrschenden Meinung ist dieser Vorgabe zwar bereits nach geltendem Recht (§ 184b Absatz 4, § 184c Absatz 4 StGB) ausreichend Rechnung getragen. Eine Klarstellung erscheint aber sinnvoll und berücksichtigt auch mögliche zukünftige technische Entwicklungen, die eine Begründung für die Verwirklichung des Besitztatbestandes erschweren würden» [Drucksache 18/2601, 34 (cfr. anche nota 138)].

[127] La *cache* (dal francese «nascondiglio») è come noto un'area di memoria ausiliaria di un elaboratore elettronico (detta in italiano «memoria nascosta»), caratterizzata da una velocità d'accesso superiore a quella della memoria principale, nella quale vengono registrati istruzioni e dati richiesti con particolare frequenza da un programma, allo scopo di aumentare la velocità di elaborazione. In sintesi i *file* vengono salvati in automatico in locale al fine di consentire una consultazione più rapida in caso di successivo accesso. Vi sono vari tipi di memoria *cache*.

[128] P. CORDERO, *op. cit.* in nota 124, 1169.

che nella giurisprudenza e dottrina straniere[129], non convince appieno e porta ad emersione le peculiarità di un contesto operativo, quello informatico, in cui si assiste ad una rarefazione della materialità fisica dei comportamenti, che impone forse di rimeditare le categorie dogmatiche tradizionali. Il procurarsi parrebbe presupporre, infatti, una componente di scopo che dovrebbe caratterizzare la condotta, un'azione tesa a raggiungere un determinato fine, quella che in tedesco si è definita «finale Zwecksetzung»[130]. L'automatizzazione del processo acquisitivo tramite l'intermediazione di un procedimento informatizzato con finalità autonome, che "rompe" la sequenza naturalistica condotta-evento, impone di interrogarsi sulla stessa configurabilità di una condotta tipica e circa l'esistenza di un dominio cosciente finalistico su di un atteggiamento che non si esaurisce in un mero atteggiamento corporeo. Il quesito diviene di particolare interesse soprattutto laddove il procurarsi o l'acquisire, come nel caso oggetto di analisi, non costituiscano condotta alternativa al detenere nell'ambito di una norma a più fattispecie o norma mista alternativa. La soluzione tradizionale, sul presupposto oggettivo del salvataggio durante la navigazione, muove da una ritenuta incontroversa ricorrenza dell'elemento oggettivo, rinviando all'indagine sull'elemento soggettivo il quesito circa l'integrazione della fattispecie. La stessa ricorrenza dell'elemento soggettivo viene poi desunta da elementi circostanziali, secondo procedimenti di inferenza logica che sollevano non poche perplessità. In particolare si afferma che la prova dell'elemento soggettivo possa derivarsi dalla conoscenza dell'esistenza di una procedura automatizzata di salvataggio, a sua volta desunta dalla cancellazione di tali *file*[131]. A riguardo va precisato che la cancellazione

[129] Cfr. BGH dd. 10.10.2006, S StR 430/06, in *Neue Zeitschrift für Strafrecht*, 2007, 95; sentenza disponibile anche *online* sul sito *www.bundesgerichtshof.de*; OLG Hamburg dell'11.11.2008 - 1 - 53/08 (REV), in *Strafverteidiger*, 2009, 469 ss., con nota di J. BURMEISTER, E. BÖHM. Sulla problematica si veda I. SALVADORI, *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata*, Napoli, 2016, 85 ss.; per riferimenti stranieri, *ibidem*, 86, nota 110.

[130] T. HÖRNLE, *op. cit.* in nota 121, 1591.

[131] P. CORDERO, *op. cit.* in nota 124, 1169: «vi è volontarietà giacché si ha la conoscenza dell'esistenza del materiale in quest'area del *computer*, conoscenza desunta dal fatto che si ha coscientemente operato per modificarla». Altre volte si è affermato che la cancellazione immediata o automatica (per impostazione predefinita dall'utente) alla

completa della cronologia non costituisce necessariamente prova della conoscenza del salvataggio di determinati *file*[132]. Le peculiarità della realtà informatica e la conoscenza media del funzionamento di tali strumenti sembrano frapporsi alla possibilità di elevare la condotta richiamata a criterio ordinario di inferenza probatoria[133] rispetto alla consapevolezza sul fatto di procurarsi/possedere-detenere determinati *file*. Seguendo l'orientamento dinnanzi richiamato, l'unico modo per potersi escludere la ricorrenza del fatto tipico sarebbe dato dalla disattivazione della funzione di salvataggio automatico. Tale soluzione pone però una serie di problematiche. *In primis* l'operazione di disattivazione non sempre risulta facilmente accessibile all'utente medio[134], imponendo un comando specifico, volto a modificare le impostazioni di *default*. In secondo luogo il salvataggio automatico dei *file* persegue uno scopo perfettamente lecito (quello di rendere la navigazione più rapida), rispetto al quale l'"acquisizione" del materiale appare funzionale. Quindi per far sì che una condotta penalmente irrilevante, per quanto deplorevole, non debba considerarsi tipica, si impone un fare attivo (quindi non si sarebbe più in presenza di un mero comando negativo), volto a disattivare una funzione automatica, connotata per scopi e natura a facilitare una condotta per l'appunto penalmente irrilevante.

Non si può certo sottacere l'eventualità di forme di manifestazione criminali volte a sfruttare funzionalità lecite per scopi illeciti e dunque la possibilità che la navigazione sia funzionale proprio all'acquisizione automatica di *file*. Tuttavia i timori di eventuali lacune di tutela, che potrebbero farsi ancor più stringenti laddove la norma, come nel caso di

---

chiusura del *browser* della *cache* escluderebbe la fattispecie, ponendosi però il quesito sulla fonte giuridica di tale obbligo di agire: T. FISCHER, *§ 184b Verbreitung*..., cit. in nota 126, 1323.

[132] Di frequente la cancellazione dei dati della navigazione avviene per mero scrupolo, soprattutto laddove si tratti di *computer* in uso a più utenti, al fine di tutelare la propria *privacy*; desumere da ciò la consapevolezza sull'acquisizione di specifici *file* durante la navigazione parrebbe operazione eccessiva.

[133] Nello stesso senso I. SALVADORI, *op. cit.* in nota 129, 87.

[134] Occorre segnalare come ormai la maggior parte dei *browser* offrano la possibilità di una navigazione anonima, volta ad escludere la memorizzazione automatica dei dati relativi alla sessione di esplorazione, inclusi *cookie*, *file* temporanei di internet, cronologia e altri dati.

specie, non punisca accanto al procacciamento anche la detenzione[135], paiono cedere il passo di fronte a preoccupazioni di salvaguardia della presunzione di innocenza nel rimettere la punibilità a valutazioni sull'elemento soggettivo alla luce di quella che, non a caso, si è definita una graduale emarginazione processuale del dolo[136], soprattutto in settori fortemente intrisi da valutazioni sul tipo di autore.

Occorre in ogni caso evidenziare, pur nell'identità degli strumenti tecnologici utilizzati, le peculiarità e l'autonomia del fenomeno terroristico, rispetto a quello della pornografia minorile, le quali inevitabilmente finiscono per incidere anche sull'analisi delle singole fattispecie e delle nozioni ivi richiamate, di modo che i rimandi legislativi impongono particolare cautela nell'indagine scientifica[137]. Lo stesso legislatore tedesco se da un lato, non solo ha dato per pacifico il procurarsi nel caso della visualizzazione *online* con contestuale salvataggio automatico nella *cache*, ma ha anche esteso la punibilità di fatto al mero tentativo di connessione a pagine internet con contenuto pedopornografico[138],

[135] In tal caso però le riserve, come si vedrà, potranno essere di tipo diverso, legate alla scelta di punire solo il procurarsi e non la visualizzazione ripetuta o continuata del materiale *online*.

[136] F.M. IACOVIELLO, *Processo di parti e prova del dolo*, in *Criminalia*, 2010, 465.

[137] Per le ragioni che precedono, pur condividendo le interessanti riflessioni sviluppate da Flor in questo volume, non riteniamo colga nel segno la critica rivolta all'adozione di argomentazioni sistematiche nell'analisi della fattispecie. All'uopo si rende opportuno precisare come il richiamo a concetti consolidati sia stato operato *in primis* dagli stessi legislatori, oltre ad essere criterio adottato da miglior dottrina italiana e straniera, ed anzi, per usare le parole di L. PICOTTI, *I delitti di sfruttamento sessuale dei bambini…*, cit. in nota 124, 1305, «è da apprezzare […] (un) approccio sistematico unitario, quando in settori pur diversi di tutela si presentino esigenze analoghe di adattamento della disciplina e delle formulazioni normative alle caratteristiche ed alle qualità tecniche dei nuovi mezzi e delle nuove procedure di trattamento automatizzato e di circolazione delle "informazioni", come in particolare accade per la comunicazione, diffusione, trasmissione per via telematica, divenute rilevanti sul piano giuridico in seguito all'espansione dell'uso di Internet». Eravamo infine noi stessi nel citato scritto ad indicare in ogni caso l'opportunità di cautela nell'analisi scientifica in ragione delle peculiarità del fenomeno oggetto di indagine.

[138] La Convenzione di Lanzarote del Consiglio d'Europa (Convenzione del Consiglio d'Europa per la protezione dei bambini contro lo sfruttamento e gli abusi sessuali STCE n. 201) all'art. 20 co. 1 lett. f) punisce espressamente l'accesso consapevole, a

ha invece ritenuto non sufficiente la mera visualizzazione *online*, con connesso salvataggio, nel caso del § 91 StGB[139], tracciando quindi un'espressa differenziazione tra le due fattispecie. Anche in Austria con riferimento al § 278f co. 2 StGB sia il legislatore[140], sia la dottrina[141]

---

mezzo di tecnologie dell'informazione e della comunicazione, a materiale pedopornografico, lasciando però agli Stati la facoltà di attuare o meno tale raccomandazione (art. 20 co. 4). La previsione è poi stata recepita dalla direttiva 2011/93/UE del parlamento europeo e del consiglio del 13 dicembre 2011 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio, la quale al pari punisce tale condotta all'art. 5 co. 3. Il legislatore tedesco al fine del recepimento della convenzione e della direttiva e dunque di colmare una possibile lacuna normativa, con legge del 21.01.2015 (*Neunundvierzigstes Gesetz zur Änderung des Strafgesetzbuches. Umsetzung europäischer Vorgaben zum Sexualstrafrecht*) ha sostituito il riferimento al procurarsi con quello della connessione (*Abruf*), la quale non richiede alcun salvataggio: «…wobei der Abruf nicht die Speicherung des Werkes bei dem Abrufenden voraussetzt» (Drucksache 18/2601, 16) e «Kinderpornographische Inhalte werden abgerufen, wenn der Nutzer die Übertragung der Daten durch Telemedien veranlasst und sich dadurch die Möglichkeit der Kenntnisnahme von ihrem Inhalt verschafft», *ibidem*, 34 (cfr. § 184d StGB) (cfr. anche nota 126). L'Italia ha ratificato la convenzione con legge 1 ottobre 2012, n. 172 e la direttiva con decreto legislativo 4 marzo 2014, n. 39. A fondamento della mancata punizione del mero accesso nella relazione del disegno di legge di conversione della Convenzione di Lanzarote (C. 2326) sono indicati dubbi di legittimità costituzionale di una tale incriminazione: «per il nostro Stato, l'esigenza di apporre la riserva discende dai dubbi di costituzionalità di una norma che sanzioni una condotta che potrebbe essere anche del tutto casuale, oltre che dalle difficoltà probatorie di una fattispecie penale che non preveda in qualche modo lo scarico (*download*) del materiale visionato» (C. 2326, 10); il legislatore italiano dovrebbe però introdurre tale incriminazione (al pari di quanto avvenuto in altri Paesi: Austria, Germania, Francia, ecc.) per dare attuazione alla direttiva citata.

[139] BT-Drucksache 16/12428, 18: «Der Begriff des Sichverschaffens setzt einen nicht nur flüchtigen, vorübergehenden Zugriff auf die Schrift voraus. Der vorübergehende Zugriff auf Daten, der z.B. mit der Anzeige der Anleitung in einem Webbrowserprogramm und den technisch bedingten Zwischenspeicherungen im Rechner verbunden ist, genügt somit nicht – anders als bei § 184b Abs. 4 Satz 1 StGB». Va all'uopo tuttavia precisato che, a differenza di quanto avviene in Austria, il § 184b StGB prevede un delitto a consumazione anticipata (*Unternehmensdelikt*), sanzionandosi la condotta di chi commette un fatto diretto a procurarsi il materiale in questione, a differenza del § 91 StGB, il quale sanziona il fatto di procurarsi i «documenti» (*Schriften*).

[140] Cfr. nota 118.

richiedono ai fini della realizzazione della condotta del procurarsi che le informazioni siano salvate su di un supporto di memoria.

In materia di terrorismo si è precisato che lo scopo degli interventi sovranazionali sarebbe di adattare la legislazione vigente ai cambiamenti del *modus operandi* degli attivisti e dei sostenitori di attività terroristiche, in particolare la sostituzione di gruppi gerarchicamente strutturati con cellule semiautonome o singoli individui, i cosiddetti «lupi solitari», e il crescente utilizzo di internet per ispirare, mobilitare e fornire istruzioni e addestramento a reti terroristiche locali e a singoli individui[142]. Gli stessi legislatori nazionali hanno evidenziato in tal senso la volontà di introdurre misure volte a contenere e a reprimere le azioni poste in essere attraverso lo strumento telematico, idoneo a raggiungere un numero sempre maggiore di potenziali combattenti e i terroristi che operano sganciati da sodalizi e da organizzazioni criminali[143]. Se dunque lo scopo del legislatore è quello di evitare che persone possano essere istigate a commettere atti di terrorismo o comunque si procurino le conoscenze necessarie a tal fine, solleva perplessità sotto il profilo della coerenza la scelta di vincolare la punibilità ad un dato materiale, quello del possesso delle informazioni, e non già a quello intellettivo dell'acquisizione delle conoscenze necessarie a perpetrare tali fatti. Rispetto alla *ratio* dell'incriminazione – salve in ogni caso le perplessità generali sull'anticipazione spinta della punibilità introdotta dalle fattispecie in commento – non si giustificherebbe quindi una differenziazione rispetto al soggetto che si limiti a visionare i *file online*, mediante continui, prolungati e ripetuti accessi; in tal modo al terrorista accorto sarebbe con-

[141] H. HINTERHOFER, C. ROSBAUD, *op. cit.* in nota 104, 321; F. PLÖCHL, *op. cit.* in nota 46, 98 e 99.

[142] Cfr. in particolare i considerando 4 e 5 della decisione quadro 2008/919/GAI, nonché la relazione della Commissione europea sull'attuazione della decisione quadro 2008/919/GAI del Consiglio, del 28 novembre 2008, che modifica la decisione quadro 202/475/GAI sulla lotta contro il terrorismo, Bruxelles, 2014, 4, disponibile sul sito *www.ec.europa.eu*.

[143] Cfr. *Terrorismuspräventionsgesetz 2010*, cit. in nota 118; il progetto di legge tedesco BT-Drucksache 16/12428 e le relazioni accompagnatorie al disegno di legge di conversione del d.l. 144/2005 (S. 3571) e del d.l. 7/2014 (C. 2893).

sentito reperire legalmente le informazioni necessarie ai suoi fini[144]. Rispetto alla disciplina normativa italiana potrebbe in tal senso "soccorrere" l'indeterminatezza e l'uso a-tecnico del termine acquisire che fra le sue varie accezioni terminologiche, accanto all'acquisto del possesso in senso materiale, comprende anche quella dell'assimilazione intellettuale, tenuto altresì conto dell'oggetto della condotta: istruzioni; al pari di quanto ad esempio avvenuto con riferimento alla condotta del procurarsi notizie prevista dagli artt. 256, 257 e 258 c.p., laddove si è fatto riferimento anche alla dimensione intellettiva del prendere cognizione, venire a conoscenza.

### *7.2. Comportamenti univocamente finalizzati alla commissione di condotte terroristiche*

Quanto emerge – in particolare nel confronto con altre realtà straniere – è lo sforzo del legislatore, a fronte dell'anticipazione spinta della punibilità a condotte potenzialmente neutre, di ancorare l'intervento sanzionatorio ad un parametro oggettivo che travalichi la mera proiezione finalistica.

[144] Con riferimento alla fattispecie tedesca (§ 91 StGB) si veda N. GAZEAS, *§ 91 Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat*, in K. LEIPOLD, M. TSAMBIKAKIS, M.A. ZÖLLER (a cura di), *op. cit.* in nota 46, 776 s.; N. GAZEAS, T. GROSSE-WILDE, A. KIEßLING, *op. cit.* in nota 96, 603. La possibile giustificazione alla differenziazione potrebbe essere legata a motivi probatori; si confronti sul punto quanto espressamente precisato dal legislatore italiano in riferimento alla non punizione della mera visualizzazione di materiale pedopornografico in ordine a condotte che non prevedano quantomeno lo scarico del materiale, cfr. nota 138. Nonostante le differenti *ratio* di tutela, non è mancato peraltro chi ha suggerito di estendere la nozione del procurarsi alla visualizzazione nel caso di ripetuti collegamenti a siti dello stesso genere, in quanto la detenzione non sarebbe condizione necessaria per la fruizione del materiale pornografico: A. COSTANZO, *I reati contro la libertà sessuale. Profili sostanziali, probatori e processuali*, Milano, 2008, 113 (modello che ad esempio si ritrova in Francia: art. 227-23, co. 4 c.p.). In tal modo si elevano a condotta, sussumendoli nel fatto tipico, elementi circostanziali dai quali solitamente si desume sotto il profilo probatorio la consapevolezza del contenuto pedopornografico dei siti o del materiale in questione; cfr. direttiva 2011/92/UE, 18° considerando: «Il carattere intenzionale del reato può dedursi in particolare dal fatto che gli accessi siano ricorrenti o che i reati siano stati commessi attraverso un servizio a pagamento».

Va evidenziato come sia stato in primo luogo oggetto di censura il ricorso "innovativo" ad un termine a-tecnico quale "comportamenti"[145]. Si tratta anche in tal caso, come per l'acquisire, di un *novum*[146] per il codice penale che tra l'altro si contraddistinguerebbe per assoluta indeterminatezza, potendovi ricadere pressoché ogni attività materiale[147]. La funzione selettiva delle condotte tipiche verrebbe quindi affidata alla dialettica processuale attraverso la ricostruzione di elementi circostanziali dai quali emergerebbe il fine delittuoso[148].

In tal senso si giustificherebbe l'introduzione del riferimento all'univocità, avvenuta in fase di conversione ad opera delle commissioni riunite in sede referente, su proposta del presidente, Donatella Ferranti, «in considerazione del fatto che l'articolo 270-sexies del codice penale non si riferisce a reati, bensì a tipi di condotte»[149], così riformulandosi gli emendamenti che proponevano originariamente di inserire accanto all'univocità anche il riferimento all'idoneità[150]. Se pur evidente la *ratio*

[145] Cfr. sul punto A. CAVALIERE, *Considerazioni critiche…*, cit. in nota 51, 8 s.; F. FASANI, *Le nuove fattispecie antiterrorismo…*, cit. in nota 51, 943; G. LEO, *op. cit*. in nota 51; A. VARVARESSOS, *op. cit.* in nota 115, 13 s.

[146] Oltre che nelle fattispecie relative al maltrattamento di animali (art. 544-*ter* c.p.), il termine in ambito penale si ritrova anche all'art. 1 (Casi di non punibilità) della l. 29 maggio 1982, n. 304 (Misure per la difesa dell'ordinamento costituzionale).

[147] A. CAVALIERE, *Considerazioni critiche…*, cit. in nota 51, 8 s.; A. VARVARESSOS, *op. cit.* in nota 115, 13 s.; F. FASANI, *Le nuove fattispecie antiterrorismo…*, cit. in nota 51, 943; ad avviso di quest'ultimo il termine sarebbe non solo indeterminato, ma anche utilizzato in maniera impropria in quanto esso si riferirebbe non ad una singola condotta, oggetto di potenziale attenzione del legislatore, quanto piuttosto al complessivo modo di comportarsi.

[148] Cfr. A. VARVARESSOS, *op. cit.* in nota 115, 13.

[149] Resoconto della seduta del 18 marzo 2015 delle Commissioni Riunite (II e IV), 8.

[150] Si tratta in particolare dell'emendamento 1.21, poi riformulato, che prevedeva di utilizzare la seguente formula «nonché della persona che avendo acquisito, anche autonomamente, le istruzioni per il compimento degli atti di cui al primo periodo, pone in essere atti idonei diretti in modo non equivoco alla commissione di reati determinati con le finalità del 270-sexies». Non trovarono accoglimento nemmeno gli emendamenti proposti successivamente in assemblea – seduta n. 400 del 26.03.2015, n. 1.201 («idonei e») e 1.205 («atti idonei diretti univocamente alla commissione di reati determinati con le finalità dell'articolo 270-*sexies*») – con i quali si mirava nuovamente ad inserire il requisito espresso dell'idoneità. Si veda in particolare l'intervento di D. Pesco, alla

sottesa all'introduzione del requisito dell'univocità, data dall'intenzione di limitare l'ambito applicativo della fattispecie in ossequio al principio di materialità[151], la portata applicativa del "correttivo", così come il suo inquadramento sistematico, soprattutto nel rapporto con altre fattispecie, sono stati oggetto di dibattito e differenti letture interpretative. Da un punto di vista della coerenza logica, parrebbe in ogni caso una contraddizione di termini il voler introdurre un criterio di selettività parametrato ad un elemento a sua volta carente sotto il profilo della determinatezza: l'incapacità selettiva del termine di riferimento ricade necessariamente sul requisito che dovrebbe essere espressione della tensione/direzione della condotta verso quell'obiettivo. Detto ciò, come già ricordato, è evidente come lo scopo sia quello di selezionare le condotte realmente meritevoli di sanzione[152].

In molti, valorizzando il requisito implicito dell'idoneità ricavato sulla scorta della lettura "correttiva" della Suprema Corte in materia di dolo specifico[153], hanno ritenuto di poter individuare nella fattispecie

---

seduta della Camera n. 402 del 31 marzo 2015, laddove questi precisava: «È necessaria […] l'emanazione di una norma che preveda la sostituzione della parola "comportamenti" con la locuzione "atti idonei diretti in modo non equivoco", mutuata dall'articolo 56 del codice penale, per conferire sia maggiore materialità che maggiore determinatezza alla fattispecie, richiamando le parole e la loro consolidata interpretazione usata dal legislatore per il delitto tentato. Infatti, sempre in ossequio a materialità e determinatezza, dopo l'addestramento subìto o autonomo, la punibilità dovrà scattare non quando vi sarà la prova di voler perseguire le finalità di cui all'articolo 270-*sexies* (Condotte con finalità di terrorismo), ma quando vi sarà la prova che l'imputato ha tentato – ripeto: ha tentato – la commissione di reati precisi (quali che siano, ma vanno individuati) animato da quelle finalità terroristiche» (Resoconto stenografico dell'Assemblea, 18).

[151] Cfr. M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione…*, cit. in nota 70, 138. Riemerge qui, nel confronto con le esperienze straniere e sovranazionali, la centralità del principio di offensività nella nostra tradizione giuridica e il ruolo sempre maggiore che esso va assumendo a fronte della graduale trasformazione del diritto penale da strumento di *extrema ratio* a tecnica di governo e di controllo di qualsivoglia fenomeno sociale.

[152] Cfr. A. VARVARESSOS, *op. cit.* in nota 115, 14: «isolare dall'insieme indeterminato delle condotte astrattamente punibili solo quelle che manifestano in concreto l'insidiosità per il bene giuridico protetto».

[153] Si veda quanto più sopra riportato; cfr. nota 69.

una sorta di tentativo "speciale"[154]. La lettura impone, tuttavia, talune precisazioni e distinguo, in ragione delle stesse indicazioni della Suprema Corte e di un criterio interpretativo storico. In primo luogo occorre evidenziare, come più sopra ricordato[155], che gli emendamenti volti ad introdurre un espresso riferimento al requisito dell'idoneità all'interno della fattispecie non trovarono accoglimento. Sotto il profilo della *voluntas legis* potrebbe indi apparire una forzatura – per quanto operazione interpretativa non certamente inedita, né infondata – l'introduzione di un requisito di idoneità implicito, salvo in ogni caso precisarsi che fu lo stesso legislatore in sede di conversione a rinviare al dolo specifico quale elemento idoneo ad assicurare la «caratterizzazione della fattispecie»[156]. Potrebbe pertanto anche ritenersi che si sia ritenuto superfluo esplicitare un requisito implicito; scelta questa, in caso, certamente criticabile, posto che un'espressa previsione normativa sarebbe stata in ogni caso preferibile[157].

Occorre poi però chiedersi se il requisito implicito dell'idoneità possa identificarsi *sic et simpliciter* con quello espresso di cui all'art. 56 c.p. A riguardo è la stessa Corte, nella più volte citata sentenza n. 29670/2011, a precisare che l'azione non deve necessariamente raggiungere la soglia del tentativo, con ciò tracciando una demarcazione negli elementi strutturali delle fattispecie:

> Verificando le predette linee interpretative, da ritenere (nonostante talora la diversità di lessico utilizzato) *ius receptum*, può dirsi, dunque, che sotto il profilo rappresentativo assume valore dirimente l'oggetto dello scopo che muove l'agente verso l'azione che diviene tipica soltanto se è riferibile ad un momento esterno da individuarsi in quel risultato specifico descritto nella prima parte dell'art. 270-*quinquies*; nel senso che tale risultato, pur ovviamente non dovendo raggiungere le soglie del tentativo, deve comprovare la serietà dell'azione rispetto al primo fine, proiettandosi all'esterno attraverso momenti concreti di corrispondenza nei confronti della fattispecie. […] Concludendo l'esame di tale aspetto

[154] Cfr. M. CAPUTO, *op. cit.* in nota 51, 94; F. FASANI, *Le nuove fattispecie antiterrorismo…*, cit. in nota 51, 944; *contra* S. COLAIOCCO, *Le nuove norme antiterrorismo…*, cit. in nota 51, 4.

[155] Cfr. nota 150.

[156] Disegno di legge di conversione (C. 2893), 6.

[157] Nello stesso senso V. REY, *op. cit.* in nota 66, 28.

> strutturale della condotta descritta dall'art. 270-*quinquies*, può, dunque, inferirsene che se, per un verso, è il fine il momento di designazione del contegno che potrebbe altrimenti essere non punibile, per un altro verso, è l'idoneità dei mezzi che fa assumere rilevanza penale al fine, non essendo, in caso contrario, ipotizzabile alcuna offesa[158].

Ora, è pur vero che la riflessione parrebbe riferirsi precipuamente al grado di sviluppo della condotta, tuttavia, se si volesse declinare il parametro con riferimento al requisito dell'idoneità degli atti rispetto alla realizzazione del fine intenzionato, quest'ultimo, secondo la lettura avanzata dalla Corte, sembrerebbe differenziarsi dall'elemento strutturale del tentativo, estendendosene la portata applicativa e arretrandosi, dunque, la soglia di punibilità ad uno stadio anticipato rispetto all'art. 56 c.p., con il risultato di investire l'interprete e la dialettica processuale del non agevole compito di ricostruire in concreto un criterio differenziale e la reale portata applicativa delle due distinte "idoneità". Dal punto di vista teorico la soluzione individuata sembrerebbe muoversi nel senso di una idoneità più vicina alla mera possibilità. Lo sforzo concreto della Corte pare in realtà essere nel senso di escludere la rilevanza di quelle condotte che per la loro assoluta inidoneità rendono inipotizzabile una qualsiasi offesa, sforzandosi al contempo di individuare un criterio dogmatico capace di tracciare un'autonomia della fattispecie rispetto al delitto tentato del quale rischierebbe altrimenti di essere un mero duplicato[159]. Ed è proprio l'individuazione dell'autonomo ambito applicativo della nuova fattispecie uno dei punti controversi su cui si è interrogata la dottrina, in particolare per quanto concerne il rapporto con gli artt. 280 ss. c.p. Si è quindi ritenuto di poter individuare una progressione criminosa nella quale la fattispecie in commento

[158] Cass. pen., Sez. VI, 20 luglio 2011 (dep. 25 luglio 2011), n. 29670, Pres. e Rel. De Roberto, cit. in nota 69. Si veda anche quanto più sopra riportato.

[159] In senso critico F. FASANI, *Le nuove fattispecie antiterrorismo…*, cit. in nota 51, 944, aveva osservato come l'introduzione dell'avverbio "univocamente", unitamente all'orientamento che legge il dolo specifico in termini di idoneità, avrebbe determinato uno snaturamento della fattispecie che ricalcherebbe ora le orme del delitto tentato, dal che conseguirebbero profonde tensioni sistematiche.

mira a punire quelle condotte meramente preparatorie sino ad oggi penalmente irrilevanti[160].

## *8. Alcune riflessioni di sintesi*

Nelle righe che precedono ci si è sforzati di evidenziare i problemi applicativi legati, per usare un termine purtroppo ormai noto, ad una legislazione spesso emergenziale[161], per lo più attuata mediante lo schema del decreto legge. Come visto si tratta di interventi normativi che tentano, talora affannosamente, di assecondare un bisogno di sicurezza espresso dalla popolazione, scossa da gravi crimini[162], che però rischiano infine di essere strabici rispetto al problema che si intende risolvere[163] e di peccare sotto il profilo della buona tecnica normativa, anche nel confronto con il dettato sovranazionale e con le soluzioni adottate da ordinamenti stranieri. In tal modo si rischia altresì di inficia-

[160] S. COLAIOCCO, *Prime osservazioni…*, cit. in nota 51, 7; ID., *Le nuove norme antiterrorismo…*, cit. in nota 51, 4; G. MARINO, *op. cit.* in nota 51, 1413 s.; V. REY, *op. cit.* in nota 66, 25 s. Per alcune riflessioni sui rapporti tra la fattispecie in commento e quelle previste dagli artt. 280 e 280-*bis* c.p. si veda A. VARVARESSOS, *op. cit.* in nota 115, 14 s.

[161] Si veda per tutti S. MOCCIA, *La perenne emergenza. Tendenze autoritarie nel sistema penale*, 2ª ed., Napoli, 2000, il quale evidenzia come ormai si possa fare riferimento ad un «"tipo emergenziale di reato". Questo viene ad affiancarsi alle tradizionali fattispecie di reato modellate in senso garantistico, formale e sostanziale, secondo gli schemi dello stato sociale di diritto. Il tipo emergenziale presenta, invece, costantemente tali caratteristiche: approssimazione, caoticità, rigorismo repressivo, sterile simbolicità. In esso, solitamente, alla caduta in termini di garanzia si abbina la modestia dei risultati sul piano dell'effettività», *ivi*, 115.

[162] Secondo un rapporto curato da Demos, Osservatorio di Pavia e Fondazione Unipolis, *Rapporto sulla sicurezza e l'insicurezza sociale in Italia e in Europa*, dal gennaio 2015 al gennaio 2016, il timore di atti terroristici è salito dal 36,7% al 43,9%. Il rapporto è disponibile all'indirizzo: *http://www.demos.it/2016/pdf/3814rapporto_sicurezza 2016.pdf*.

[163] In senso critico si evidenzia che «l'insicurezza genera bisogno di protezione, sul quale si fondano le fortune elettorali di molti oltre che le strategie di sicurezza degli Stati» (G. ZACCARO, *Introduzione*, in *Terrorismo internazionale. Politiche della sicurezza. Diritti fondamentali*, *Edizione speciale QG*, settembre 2016, 5).

re quel percorso di armonizzazione[164] che rappresenta il presupposto indefettibile per una funzionale strategia di contrasto a fenomeni che hanno fatto della "universalità" il loro tratto caratterizzante, sia da un punto di vista criminologico, sia per quanto concerne i mezzi di cui essi si servono, in particolare la rete informatica globale.

Sintomatico rispetto allo strabismo evocato parrebbe anche il costante ricorso alle aggravanti con riferimento all'utilizzo del mezzo informatico e telematico.

### *8.1. Il ricorso alle aggravanti dell'utilizzo del mezzo informatico e telematico*

Con riferimento alle condotte di cui all'art. 270-*quinquies* con il decreto legge 18 febbraio 2015 n. 7, si è previsto un aumento di pena laddove il fatto sia commesso attraverso strumenti informatici o telematici. In sede di conversione l'aumento fu poi limitato al solo soggetto attivo e, dunque, a chi addestra o istruisce[165].

La *ratio* dell'aggravamento sarebbe da ricercarsi nella particolare insidia del ricorso a tali mezzi, che si dice diventa un'altra arma in mano ai terroristi che la utilizzano per alimentare il clima di terrore e per reclutare nuovi sostenitori[166] e nella capacità diffusiva di tali mezzi[167].

La modifica troverebbe dunque giustificazione nel sempre maggiore utilizzo di tale mezzo di comunicazione nell'ambito delle condotte in commento. Tuttavia, non si possono sottacere alcune fondate critiche di

[164] Ad avviso di I.J. PATRONE, *La legislazione dell'Unione europea tra esigenze di armonizzazione e logiche emergenziali*, in *Terrorismo internazionale. Politiche della sicurezza. Diritti fondamentali*, *Edizione speciale QG*, settembre 2016, 288 s., la stessa «legislazione europea del 2002-2008 in materia di contrasto penale al terrorismo è largamente rimasta sul terreno del diritto penale simbolico, senza riuscire veramente ad incidere sui sistemi nazionali, armonizzandoli solo in parte e molto lentamente».

[165] Emendamento 1.26 approvato dalle Commissioni riunite, si veda il Resoconto della seduta del 18 marzo 2015 delle Commissioni Riunite (II e IV), 10 s.

[166] Disegno di legge di conversione (C. 2893), 7. Il passo in realtà si riferisce più precisamente alla medesima aggravante inserita con riferimento agli artt. 302 e 404 c.p., espressamente richiamata per motivi di coerenza a giustificazione dell'introduzione della medesima aggravante con riferimento all'art. 270-*quinquies* c.p.

[167] *Dossier* del Servizio Studi del Senato sull'A.S. n. 1854, aprile 2015 n. 204, 25.

varia natura che l'introduzione dell'aggravante solleva con riferimento alla fattispecie in commento.

In primo luogo si osserva come sotto il profilo dell'offensività l'aggravamento possa apparire ingiustificato e frutto di una fuorviante suggestione casistica[168], così traducendosi «– secondo cadenze proprie di un fiscale contrappasso a fini simbolico-repressivi – qualsiasi sfumatura casistica, emotivamente allarmante, di un fatto in mesi ed anni di ulteriore pena detentiva»[169]; non vi sarebbe, ad avviso di taluni autori, alcuna riflessione di matrice politico-criminale, tendente allo sviluppo delle tradizionali funzioni delle circostanze in relazione all'individualizzazione della pena rispetto alla gravità del fatto, alla colpevolezza del soggetto agente e alla sua pericolosità[170].

In particolare ci si è chiesti[171] in cosa consista la maggiore insidiosità che dovrebbe giustificare l'aggravamento sanzionatorio: qual è la maggior offesa connessa alla condotta realizzata mediante l'interposizione di uno strumento informatico rispetto ad un addestramento che avvenga tramite un contatto diretto nella contestuale presenza fisica del maestro e dell'allievo? Non si può che osservare che anzi in tal caso il buon esito dell'addestramento risulterà facilitato dalla possibilità di un'interazione diretta. Discorso diverso andrebbe fatto per quanto concerne la diffusione delle informazioni, ma in tal caso per giustificare l'aggravamento sarebbe stato opportuno condizionare la condotta ad un'idoneità istigatoria della stessa e quindi alle modalità concrete di

[168] A. CAVALIERE, *Considerazioni critiche…*, cit. in nota 51, 12; F. FASANI, *Le nuove fattispecie antiterrorismo…*, cit. in nota 51, 945.

[169] A. CAVALIERE, *Considerazioni critiche…*, cit. in nota 51, 12. Nello stesso senso A. PECCIOLI, *op. cit.* in nota 20, 774: «La previsione di circostanze aggravanti è una costante nei provvedimenti in cui il legislatore, negli anni passati, ha tentato di porre rimedio ad eventi di natura eccezionale ed emergenziali in grado di incidere negativamente sull'ordine pubblico e sulla sicurezza pubblica».

[170] F. FASANI, *Le nuove fattispecie antiterrorismo…*, cit. in nota 51, 945; G. CARLINO, *Dalla normativa penale antiterrorismo alcune deduzioni democratico-costituzionali*, in *Sicurezza, Terrorismo e Società*, n. 3, 2016, 155 s.

[171] A. CAVALIERE, *Considerazioni critiche…*, cit. in nota 51, 12; F. FASANI, *Le nuove fattispecie antiterrorismo…*, cit. in nota 51, 945.

diffusione, stante l'amplissima, e di fatto incontrollata, presenza di tali informazioni in rete[172].

La giustificazione dell'aggravamento parrebbe allora doversi ricercare, come detto, in una suggestione casistica, legata al sempre più frequente utilizzo degli strumenti in oggetto, e dunque al fine di una più efficace strategia di contrasto.

A riguardo, tuttavia, si pone la seconda delle critiche, ossia quella circa l'effettiva utilità di una siffatta previsione, che rischia di colorarsi di sterile simbolicità. Proprio la natura delocalizzata degli strumenti in commento fa sì che gli autori materiali delle condotte di addestramento, come anche nel caso del proselitismo, si trovino fisicamente all'estero, spesso in territori di conflitto e quindi con limitate possibilità di una reale punizione. Se poi si considera che la circostanza aggravante si applica solo al soggetto attivo, sarà assai agevole «aggirarne» la portata applicativa, scaricando i *file* in remoto e diffondendoli materialmente su supporto digitale (CD, DVD o anche stampandolo su carta), così rompendo la «catena diffusiva telematica».

In senso contrario si osserva invece come nella normalità dei casi lo strumento informatico o telematico agevolerebbe massimamente la comunicazione, accrescendo l'offesa o il pericolo in modo esponenziale, spetterebbe poi al giudice del caso concreto valutare la reale portata offensiva dell'ausilio informatico nella vicenda sottoposta, potendosi ricorrere eventualmente ad un giudizio di bilanciamento con circostanze attenuanti (se presenti)[173]. Pur non potendosi che condividere la riflessione in punto potenziale diffusivo dello strumento – salvo quanto più sopra evidenziato –, la valutazione in concreto dell'offesa avrebbe a nostro avviso potuto svolgersi in ogni caso servendosi degli ordinari criteri di commisurazione della pena di cui all'art. 133 c.p., tenuto in particolare conto dell'ampia cornice edittale (da 5 a 10 anni di reclusione) all'interno della quale al giudice è dato di muoversi al fine di parametrare la pena al concreto disvalore del fatto. In tal modo si sarebbe altresì potuto evitare quello che in sede parlamentare si è definito un

[172] A riguardo non si può che rinviare a quanto più sopra esposto, prendendo spunto dalle esperienze straniere.

[173] C.D. LEOTTA, *op. cit.* in nota 51, 7.

«atteggiamento ostile nei riguardi dell'utilizzo degli strumenti informatici»[174].

### *8.2. La "trasformazione" del diritto penale classico*

Come si è da più parti evidenziato, appare evidente come lo scopo precipuo delle incriminazioni in commento sia da un lato quello di rompere il ruolo tipizzante del vincolo associativo, così da supplire ad eventuali deficit probatori, che spesso l'accusa incontra[175], e dall'altro di sottoporre a pena condotte prodromiche a gravi fatti di reato[176].

Da quanto precede emerge chiaramente come il diritto penale si stia sempre più discostando dai paradigmi classici di ispirazione liberale del *post factum* per assumere funzioni di prevenzione in un'ottica di neutralizzazione *ante factum* e dunque di polizia in senso stretto, in cui l'attenzione viene spostata sulla necessità «di una risposta preventiva accentuata, che controlli alla radice le fonti di rischio, piuttosto che i pericoli concreti»[177]. In realtà, si è acutamente osservato come si tratterebbe di una classica forma di tutela propria del diritto penale politico di cui le norme penali anti-terrorismo non sarebbero che l'espressione moderna[178].

Se da un lato l'enorme potenzialità lesiva dei reati "minacciati" pare costituire idoneo supporto cui ancorare il giudizio di legittimità dell'intervento normativo, dall'altro riemerge con forza il quesito circa la tollerabilità di una così spinta «anticipazione della tutela penale, a fronte di fattispecie che incriminano atti sempre più distanti, dal punto di vista

[174] Cosi si era espresso A. Tofalo nel corso della seduta del 18 marzo 2015 delle Commissioni Riunite (II e IV); si veda il Resoconto della seduta, 10 s.

[175] Le norme vanno, infatti, a punire comportamenti ritenuti sintomatici dell'esistenza di organizzazioni terroristiche, senza necessità di doverne fornire la dimostrazione: L. PISTORELLI, *op. cit.* in nota 18, 56; M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione*..., cit. in nota 70, 139 s.; G. LEO, *op. cit*. in nota 51; M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale*, cit. in nota 70, 109.

[176] F. VIGANÒ, *Minaccia dei 'lupi solitari'*..., cit. nota 14, XI.

[177] M. DONINI, *Sicurezza e diritto penale*, cit. in nota 26, 3561.

[178] M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale*, cit. in nota 70, 101.

cronologico, dalla lesione dei beni giuridici che si realizza mediante il reato 'fine' terroristico»[179].

Sono proprio queste le peculiarità di quello che si è definito un "diritto penale al limite"[180] o che potremmo definire, con una diversa scelta terminologica, un "diritto penale di frontiera": un diritto penale in bilico che si muove alla costante ricerca di un delicato equilibrio tra esigenze di "difesa" e il rischio di una compressione illegittima di diritti e libertà fondamentali. Tali peculiarità consistono per l'appunto nell'ampliamento dell'intervento penale, tramite l'incriminazione di condotte prodromiche e la rimessione alla magistratura di una funzione di controllo su possibili degenerazioni e sullo sconfinamento nel terreno della delegittimazione[181]:

> Questa è dunque la legge di un diritto penale di polizia, dove il fatto è espressione dell'autore. E la magistratura ne interpreta i percorsi per

[179] F. VIGANÒ, *Minaccia dei 'lupi solitari'...*, cit. nota 14, XI. Cfr. G. MARINUCCI, *Soggettivismo e oggettivismo nel diritto penale. Uno schizzo dogmatico e politico-criminale*, in *Riv. it. dir. proc. pen.*, 2011, 1 ss.; F. VIGANÒ, *Incriminazione di atti preparatori e principi costituzionali di garanzia nella vigente legislazione antiterrorismo*, in *ius17@unibo.it*, 2009, 171 ss. Molto critico sul punto A. CAVALIERE, *Le nuove emergenze terroristiche: il difficile rapporto tra esigenze di tutela e garanzie individuali*, in questo volume.

[180] L'espressione è di M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale*, cit. in nota 70, 99 ss., che la utilizza per differenziare tale diritto penale dal "diritto penale del nemico" e per descrivere «scelte di politica penale nelle quali principi e garanzie proprie del diritto penale subiscono flessibilizzazioni che si muovono comunque in un'area limitrofa ad un confine pericoloso, quello al di là del quale si vanificano, in nome della ragion di Stato, garanzie e diritti individuali sui quali si fonda l'ordinamento democratico. È un diritto penale, dunque, legittimo, ma che si muove in un'area dove è sempre alto il rischio che la ragionevolezza delle scelte di incriminazione, delle strategie processuali e delle misure preventive si traduca in forme illegittime di violazione di diritti e libertà fondamentali, perché in tal caso lo Stato di diritto negherebbe se stesso», *ivi*, 100 s.

[181] Nello stesso senso, per l'appunto, M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale*, cit. in nota 70, 101; il quale acutamente osserva ancora che «proprio nelle fattispecie a struttura fortemente anticipata si annida il progressivo avvicinamento del diritto penale del limite verso il confine della sua delegittimazione», *ivi*, 110.

prevenire la consumazione di stragi e attentati. L'abbiamo camuffato da diritto penale del fatto, ma siamo già oltre i suoi confini[182].

### *8.2.1. Quale ruolo per la magistratura?*

La richiamata frenesia interventistica parrebbe dunque dare luogo a paradossi applicativi, rischi di delegittimazione dello strumento penale, incoerenze e lacune colmabili solo a livello interpretativo, riversando tale compito sul potere giudiziario[183].

In tal modo, però, vi è il rischio di attribuire alla magistratura un compito che non dovrebbe spettarle, dando vita ad una sua crisi di identità, giacché, per usare le parole proferite da Vitaliano Esposito all'inaugurazione dell'anno giudiziario 2009, il magistrato che applichi una norma priva dei requisiti di chiarezza, accessibilità e prevedibilità nei suoi effetti, viola il principio della sicurezza giuridica dei cittadini, che è un principio cardine di ogni società democratica[184].

La perdita di capacità selettiva della fattispecie, l'alleggerimento dell'onere probatorio necessario a supportare l'imputazione, la rottura del ruolo tipizzante del vincolo associativo, un disvalore del fatto incentrato sulla proiezione finalistica, sulla volontà di scopo, portano ad emersione il rischio che la norma, come già ricordato, possa divenire un «mero strumento di legittimazione legalistica di una scelta repressiva concreta»[185].

---

[182] M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione*…, cit. in nota 70, 140 s.

[183] Circostanza di cui la stessa magistratura parrebbe ben consapevole, come evidenziato dal parere emesso dal CSM riguardante il decreto legge n. 7/2015, laddove, proprio con riferimento all'art. 270-*quinquies* c.p., si precisa che la norma «comporta un inedito arretramento della soglia della rilevanza penale sino al compimento di atti meramente preparatori, che interpellerà la capacità dell'interprete di assicurare il rispetto del principio di necessaria offensività della condotta», Delibera consiliare del 18 marzo 2015.

[184] V. ESPOSITO, *Intervento del Procuratore Generale della Corte Suprema di Cassazione*, Roma, 30 gennaio 2009, 2 s.; testo disponibile sul sito della Suprema Corte di Cassazione.

[185] Cfr. nota 84. Cfr. sul punto anche G. CARLINO, *op. cit.* in nota 170, 154, 160 s.

Va a tal riguardo, tuttavia, precisato che, come si è acutamente osservato, la funzione delle incriminazioni in commento si pone essenzialmente non nell'ambito dell'accertamento ed ascrizione di una responsabilità penale, bensì, a fronte della gravità della lesione minacciata, in un'ottica di neutralizzazione preventiva e quindi essenzialmente in fase d'indagine:

> Le nuove norme […] servono alle indagini, *per smascherare terroristi potenziali o in pectore*. Servono per indagarli quando si ha il sospetto che abbiano intenzione di diventare i terroristi che ancora non sono. […] ogni norma incriminatrice può essere vista in una duplice dimensione: quella delle indagini e quella del dibattimento. *Come se esistessero due codici penali differenziati per fasi processuali.* Per le indagini i fatti tipici in essi previsti sono solo "indizi" o gravi indizi di quei fatti. Sono fatti anticipati. *Solo nel "codice per il dibattimento" o per il "giudizio", quei fatti sono veramente quelli di cui trattano i commenti*[186].

È il caso di ricordare, tuttavia, che «prevenzione e repressione dovrebbero obbedire a logiche diverse»[187], mentre il legislatore tende a omologarle sotto il profilo dell'afflittività, finendo talora addirittura per 'amministrativizzare' il penale, attribuendo, in presenza dei soli evanescenti parametri di pericolosità e del sospetto, al potere amministrativo/esecutivo/politico molta della violenza e della forza che caratterizza gli strumenti penali[188].

La magistratura assume dunque ad avviso di Donini una funzione di polizia, proprio in quanto le incriminazioni in commento costituiscono fattispecie ultra-preparatorie che «oggettivano in forme normative lo

---

[186] M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione…*, cit. in nota 70, 127. Sul punto si veda anche P.P. PAULESU, *Contrasto al terrorismo e presunzione di non colpevolezza*, in *Riv. dir. proc.*, 2008, 623 ss.

[187] R.E. KOSTORIS, *Il nuovo 'pacchetto' antiterrorismo, tra prevenzione, contrasto in rete e centralizzazione delle indagini*, in R.E. KOSTORIS, F. VIGANÒ (a cura di), *op. cit.* in nota 14, XVI.

[188] *Ibidem*. L'autore parla altresì di un inestricabile intreccio tra repressione e prevenzione, soprattutto laddove il diritto penale non si limiti a punire le sole azioni del passato, ma anche situazioni di pericolo.

scopo di neutralizzare soggetti molto prima dei fatti da quelli commessi»[189].

A riguardo occorre osservare come la giurisprudenza abbia mostrato in questi anni una particolare sensibilità nel ripudiare degenerazioni sistemiche, ergendosi spesso a garante dei diritti fondamentali[190], ma la difesa della democrazia, com'è stato precisato[191], impone al contempo «una sfiducia istituzionalizzata», e il genoma del penalista vede nel vincolo della norma un baluardo a difesa della libertà: «la determinatezza non è una *pruderie* da intellettuali né da professori, ma è una garanzia essenziale di difesa della libertà è, innanzitutto, difesa dal possibile arbitrio giudiziale»[192].

---

[189] M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione…*, cit. in nota 70, 127.

[190] La giurisprudenza ha mostrato la sua "resistenza" nel ripudiare un'eccessiva anticipazione della punibilità, sforzandosi di individuare parametri concreti di pericolosità, in ossequio al principio di offensività. In tal senso si valuti lo sforzo profuso, proprio con riferimento al delitto di cui all'art. 270-*quinquies* c.p., nella sentenza Cass. pen. 29670/11, cit. in nota 69, per ancorare la punibilità ad una «oggettiva idoneità della condotta a realizzare l'evento costituente l'obiettivo della condotta»; mentre è stata oggetto di censura la scelta di sanzionare il tentativo di arruolamento con riferimento all'art. 270-*quater* c.p. (Cass. pen. n. 40699/2015, cit. in nota 70), cfr. M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione…*, cit. in nota 70, 136 s.; M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale*, cit. in nota 70, 110 ss. Per altre riflessioni sul punto si veda F. VIGANÒ, *Diritto penale del nemico e diritti fondamentali*, in A. BERNARDI, B. PASTORE, A. PUGIOTTO (a cura di), *op. cit.* in nota 83, 140; A. SPATARO, *Politiche della sicurezza e diritti fondamentali*, in *Terrorismo internazionale. Politiche della sicurezza. Diritti fondamentali*, *Edizione speciale QG*, settembre 2016, 174, *passim*; M. PERROTTI, G. SPINELLI, *Punizione e legalità nel diritto penale italiano. Primi appunti per un confronto in chiave storica*, in *Cass. pen.*, 2014, 2323; questi ultimi invocano per la giurisdizione un fondamentale ruolo di "contenimento", attraverso la rigorosa valutazione di conformità del precetto a Costituzione, «onde evitare che si crei una sistematica prevalenza dello stato di necessità sulla legalità».

[191] Cfr. S. MOCCIA, *Brevi note in materia di prassi dei diritti fondamentali*, in ID. (a cura di), *op. cit.* in nota 18, 158, richiamandosi a Max Weber e Habermas.

[192] *Ibidem*, 158. E poi, come ci ricordava G. DELITALA, *Criteri direttivi del nuovo codice penale*, in ID., *Diritto penale. Raccolta degli scritti*, I, Milano, 1976, 343, nel soffermarsi sul divieto di analogia in materia penale, «un po' di diffidenza verso i giudici, in materia penale, non è neppure irrispettosa. La gravità della sanzione, che colpi-

Si è evidenziato come al momento sussisterebbero poche possibilità di rifuggire dall'uso di un "diritto penale di frontiera", stante la necessità di contrastare fenomeni criminali particolarmente invasivi e pericolosi[193], anche perché gli obblighi di incriminazione discendono da fonti sovranazionali[194]; si afferma indi che gli

> anticorpi devono, dunque, passare attraverso l'interpretazione giurisprudenziale. […] In un contesto sempre più convulso di politica criminale, per lo più mossa da spinte emergenziali, spetta alla magistratura un compito gravoso, ma ineludibile di evitare che le ansie preventive permeino anche l'interpretazione delle norme, travolgendo lo stato di diritto[195].

Se da un lato si osserva dunque il ruolo imprescindibile della magistratura nella sua "funzione contenitiva"[196], dall'altro occorre rimarcare la necessità che essa non si perverta in quanto «chiamata a svolgere

---

sce nella vita, nella libertà, nell'onore, nei beni più preziosi e sacri, la giustifica appieno».

[193] Così anche F. VIGANÒ, *Incriminazione di atti preparatori*..., cit. in nota 179, 188.

[194] Molto critico a riguardo A. CAVALIERE in questo volume laddove evidenzia il rischio che le Costituzioni nazionali e le loro garanzie fondamentali soccombano rispetto ad una normativa penale europea, con conseguente inaccettabile livellamento verso il basso delle garanzie costituzionali e conservazione solo del minimo condiviso da tutti.

[195] M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale*, cit. in nota 70, 112. Fondamentale, come ci ricorda A. CAVALIERE in questo volume, diviene in ogni caso il ruolo della dommatica, chiamata a contribuire ad un faticoso lavoro di elaborazione teorica nel fornire gli strumenti concettuali atti ad orientare la giurisprudenza.

[196] Il che imporrebbe però anche di interrogarsi in maniera critica e consapevole sull'attuale vigenza degli schemi di equilibrio, compromesso e reciproco controllo fra poteri che ispirano il modello di pensiero liberale. Cfr. sul punto quanto riportato in nota 83, in particolare la necessità evidenziata da P. MOROSINI di «una riflessione di fondo sulla impostazione culturale e sul ruolo della giurisdizione nel circuito democratico in epoche di emergenza criminale», urgendo non da ultimo, in relazione al ruolo e alla funzione che si voglia attribuire alla giurisdizione, una riflessione, altresì, sulle procedure e modalità di accesso alla stessa.

*funzioni che non le sono proprie*»[197], di fronte al rischio di una "militarizzazione" dello strumento giuridico-penale, giacché, se il diritto divenisse uno strumento di lotta, ciò implicherebbe una domanda da parte dello Stato ai giudici di «attuare le finalità di lotta che ispirano le regole da applicare. E se i giudici lottano anch'essi, va da sé che rischiano di perdere la terzietà richiesta alla funzione giurisdizionale»[198].

Ancora si è precisato che

> affidare alla *magistratura* troppe risposte ne segna inevitabilmente il destino di sovraesposizione istituzionale, funzionale all'assenza di scelte da parte del potere legislativo. Il suo successo, in questo contesto, rischia come sempre di essere direttamente proporzionale alla debolezza della politica. E dunque la sua funzione minaccia di non essere strettamente giurisdizionale, a causa di quella debolezza[199].

Ma occorre in senso realistico interrogarsi su quale possa essere la concreta alternativa[200], forse non quella dell'eccezione normativa a diritti fondamentali, posto peraltro che l'esperienza legislativa italiana ha dimostrato come tutte le deroghe temporanee rischino, infine, di divenire definitive[201], forse una maggiore presa di coscienza dei limiti del di-

---

[197] M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione*..., cit. in nota 70, 134.

[198] M. DONINI, *Lo* status *di terrorista*..., cit. in nota 83, 89. Cfr. quanto già riportato in nota 83. Precisa M. DONINI, *Il diritto penale di fronte al "nemico"*..., cit. in nota 83, 102, che «il giudice è sollecitato *contemporaneamente* ad attuare un programma di lotta nel presente e per il futuro, e ad emettere un *dictum* "imparziale" su violazioni passate». Sul punto si veda anche G. CARLINO, *op. cit.* in nota 170, 150. Critico sull'affermazione A. SPATARO, *op. cit.* in nota 190, 174. Con riferimento all'esperienza britannica, in un articolo pubblicato sul *The Guardian* nel dicembre del 2002, C. GEARTY, *Cry freedom*, evidenziava criticamente: «Only liberal idealists and others with no sense of British history expect the judicial branch to lead society in times of crisis».

[199] M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione*..., cit. in nota 70, 143, il quale individua una prima via d'uscita nella chiara delimitazione dei compiti della politica e della giurisdizione.

[200] Cfr. G. ZACCARO, *op. cit.* in nota 163, 5, richiamandosi al contributo di U. CURI, *I figli di Ares. Guerra infinita e terrorismo*, Roma, 2016.

[201] Cfr. M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione*..., cit. in nota 70, 141.

ritto penale, soprattutto laddove abbandonato a se stesso[202], e dei pericoli legati ad un suo utilizzo improprio; in tal senso, come si è osservato, la disciplina del terrorismo non pare una vera eccezione allo spirito del tempo, mentre ne è conclamata la sua pericolosità come fenomeno attuale, e non potenziale, a differenza di altri ambiti della politica criminale e penale[203].

Rimane, infine, la consapevolezza, forse anche banale, ma quanto mai attuale, soprattutto in riferimento alla minaccia del terrorismo, che «se, dunque, si vuole un mondo più sicuro, è necessario costruire un mondo più giusto»[204]. Come si è rettamente osservato

> in un pianeta globalizzato negativamente è impossibile ottenere la sicurezza, e tanto mento garantirla, all'interno di un solo paese o di un gruppo scelto di paesi: non con i propri mezzi, e non a prescindere da quanto accade nel resto del mondo[205].

Senza che al contempo possa sottacersi la grave crisi che sta attraversando la moderna società: «il nuovo individualismo, l'affievolirsi dei legami umani e l'inaridirsi della solidarietà sono incisi sulla faccia di una moneta che nel suo *verso* mostra i contorni nebulosi della globalizzazione negativa»[206].

Si assiste a quello che in altra sede ho definito isolamento tecnologico[207], espressione di un paradosso che ha fatto della connettività sociale l'obiettivo dichiarato, ma che di fatto ha spezzato i legami ispirati ai

---

[202] Cfr. F. MANTOVANI, *Il vero «diritto penale minimo»: la riduzione della criminalità?*, in *Riv. it. dir. proc. pen.*, 2005, 864 ss. laddove ci ricorda che l'attuale crisi della legalità nasce da un fenomeno di anomia collettiva, cioè una perdita di valore della *norma agendi*, di "devalorizzazione" dei vari sistemi normativi, giuridici ed extragiuridici e che, dunque, la vera via per la riduzione del diritto penale non può che passare attraverso l'impegno culturale per la riduzione della criminalità.

[203] M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione…*, cit. in nota 70, 144.

[204] G. ZACCARO, *op. cit.* in nota 163, 5.

[205] Z. BAUMAN, *Il demone della paura*, Roma-Bari, 2014, 4 s.; il quale definisce la globalizzazione negativa come un processo parassitario e predatorio, che si nutre della forza succhiata dai corpi degli Stato-nazione e dei loro sudditi.

[206] *Ibidem*, 5.

[207] R. WENIN, *Disposizioni sull'addestramento…*, cit. in nota 13, 1924, nota 106.

valori della società tradizionale, dietro la spinta di pressioni di natura prettamente economica[208], cui si unisce un processo di graduale "adiaforizzazione", intesa quale affrancamento delle azioni da una valutazione etica resa possibile dall'uso di strumenti tecnici[209].

E forse non è un caso se, come ci ricorda Guido Salvini in questo volume, per "costruire" un militante regolare le Brigate Rosse e le organizzazioni similari impiegavano anni, mentre la realtà odierna mostra radicalizzazioni[210] improvvise che maturano nel giro di pochi giorni come un'infezione.

È più facile riempire un otre vuoto senza doverlo prima svuotare.

La mancanza di valori, l'autismo e l'abbandono sociale hanno reso il terreno fertile.

### *8.3. Vegliate, dunque*

Delle numerose pagine che ho letto in questi anni di ricerca sul terrorismo, continuano a risuonare nella mia mente come un mantra alcune frasi che esprimono con magistrale capacità di sintesi i contrapposti interessi in gioco.

Da un lato la consapevolezza che il terrorismo rappresenta una minaccia reale e concreta: «Nessuna "anima bella" può sottovalutare la gravità del *terrorismo* internazionale»[211].

---

[208] Si è altresì evidenziato in tal senso il paradosso di una nuova ideologia delle libertà, quella che Kant chiamava "libertà selvaggia", che mediante l'abolizione o l'allentamento dei vincoli normativi mira a conquistare ogni spazio delle relazioni sociali e attrarre nella sfera del mercato ogni tipo di beni, persino i diritti di libertà: M. BOVERO, *Premessa. Il fantasma della libertà*, in ID. (a cura di), *Quale libertà. Dizionario minimo contro i falsi liberali*, Roma-Bari, 2004, VII s.

[209] Secondo la definizione data da David Lyon, richiamandosi al concetto elaborato da Zygmunt Bauman, Z. BAUMAN, D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, Roma-Bari, 2015, 126.

[210] Cfr. sulle motivazioni del singolo terrorista F. FASANI, *Terrorismo islamico e diritto penale*, cit. in nota 2, 97.

[211] G. MARINUCCI, *Soggettivismo e oggettivismo nel diritto penale…*, cit. in nota 179, 22. L'autore prosegue la riflessione evidenziando che le norme destinate a reprimere il terrorismo non possono in ogni caso travalicare i limiti della Costituzione; anche arretrando in via d'eccezione la soglia della repressione allo stadio degli atti prepa-

La gravità della minaccia e dell'offesa arrecata impone nei fatti un arretramento della soglia di rilevanza penale a condotte meramente prodromiche, cui si lega la necessità di maggiori controlli, soprattutto nel contesto della rete.

La seconda frase è di Stefano Rodotà e ci ammonisce sul fatto che

> l'"uomo di vetro" è, storicamente, metafora totalitaria perché, reso un omaggio di facciata alle virtù civiche, nella realtà lascia il cittadino inerme di fronte a chiunque voglia impadronirsi di qualsiasi informazione che lo riguardi. Anzi, proprio adottando l'argomento del buon cittadino che nulla ha da nascondere, si fa divenire automaticamente sospetto chiunque voglia mantenere una sfera di riservatezza, intimità, libertà[212].

«La privacy come libertà dal controllo è condizione della democrazia e del pluralismo, presupposto di dignità e garanzia contro ogni discriminazione»[213].

Come ci ricorda Massimo Donini

> L'ossessione e le ragioni della sicurezza come orizzonte totalizzante del diritto penale ci portano progressivamente, senza averlo disegnato in anticipo, al prodotto collettivo di una legislazione pre-orwelliana, dalle misure di prevenzione a quelle penali, agli interventi sul controllo dei dati informatici[214].

In questi momenti di crisi, il compito sarà dunque quello di trovare il giusto compromesso tra tali due esigenze, vigilando affinché la retorica sulla necessità di controlli non finisca per sacrificare una quota ec-

---

ratori, i principi costituzionali di proporzione e offensività rappresentano limiti invalicabili a quell'arretramento.

[212] S. RODOTÀ, *Libertà personale. Vecchi e nuovi nemici*, in M. BOVERO (a cura di), *op. cit.* in nota 208, 59.

[213] Dall'intervento di A. SORO, *La società sorvegliata. I nuovi confini della libertà. Atti del convegno 28 gennaio 2016*, Roma, 2016, 5.

[214] M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione…*, cit. in nota 70, 144. Si evidenzia altresì come la sicurezza avrebbe assunto le sembianze di un'attività orientata al futuro, basata sulla sorveglianza di tutto ciò che accade e si muove (prodotti, informazioni, capitali, esseri umani): così David Lyon, in Z. BAUMAN, D. LYON, *op. cit.* in nota 209, XIII s.

cessiva di libertà in nome di una sicurezza che in realtà, talora, risulta essere solo apparente[215].

Di fronte a un'insicurezza diffusa in cui si afferma la tentazione di edificare muri tra individui e popoli, cedendo spazi di libertà all'uomo forte di turno[216], la funzione del giurista rimane quella «di sorvegliare *la tutela dei diritti fondamentali dalla stessa democrazia penale e dalle politiche internazionali*»[217].

Vegliamo, dunque…

[215] Così F. CHIUSI in occasione del *Festival Vicino/Lontano Digital 2015. Internet, terrorismo e democrazia: l'arte sottile del controllo pervasivo*, tenutosi a Udine dal 7 al 10 maggio 2015.

[216] Z. BAUMAN, nell'intervista pubblicata sul *Corriere della Sera*, 27 luglio 2016; richiamata anche da G. ZACCARO, *op. cit.* in nota 163, 6.

[217] M. DONINI, *Lotta al terrorismo e ruolo della giurisdizione*..., cit. in nota 70, 211.

*Il terrorismo transnazionale sguazza e si immerge nelle frammentate e caotiche correnti del cambiamento. E i propri martiri rappresentano i «…vinti che la corrente ha deposti sulla riva, dopo averli travolti e annegati, ciascuno colle stimmate del suo peccato, che avrebbero dovuto essere lo sfolgorare della sua virtù»* (mutuando le espressioni di Verga nella sua Prefazione a *I Malavoglia*, Milano, 19 gennaio 1881).

# MODERNITÀ ED EFFETTI COLLATERALI: IL BRODO DI COLTURA DEL TERRORISMO ISLAMICO

*Mariateresa Fiocca*

SOMMARIO: *1. Introduzione. 2. Di quale guerra parliamo? 2.1. Un prisma dalle molte sfaccettature. 2.2. Terrorismo e corruzione. 2.3. Non c'è guerra senza economia (e non c'è economia senza guerra). 3. L'innovatività della* jihād *di seconda generazione. 3.1. Il proselitismo. 4. L'innovatività delle fonti di finanziamento del Califfato. 5. L'economia della paura: una paura "liquida". 5.1. Le abitudini di consumo. 6. Le contro-misure di mitigazione del rischio di natura finanziaria: l'attività del FATF-GAFI. 7. Conclusioni.*

## *1. Introduzione*[1]

Nel presente lavoro, l'economia fa da sfondo alla lettura del terrorismo transnazionale di matrice islamica e ne rappresenta il filo rosso.

[1] Il lavoro si basa su fatti e norme all'1 ottobre 2015.

Le opinioni qui espresse sono del tutto personali e non legano l'Istituzione di appartenenza.

Indicheremo questa nuova violenta recrudescenza come "*jihād* di seconda generazione", per distinguerla – nei suoi tratti più peculiari – da quella di bin Laden e al-Zarqawi.

Il paragrafo 1 analizza la molteplice natura dell'attuale guerra. Il successivo esamina l'innovatività dell'attuale *jihād* rispetto a quella di "prima generazione", nonché i legami fra terrorismo, criminalità e corruzione. Il paragrafo 3 si concentra sulle inedite fonti di finanziamento di questo terrorismo. Il paragrafo successivo valuta le ricadute economiche della "paura-terrorismo", in particolare secondo l'approccio della *Fear Theory*. Il paragrafo 5 fornisce una breve panoramica sulle contromisure di mitigazione del rischio di natura finanziaria, facendo riferimento specificatamente all'attività del FATF-GAFI. Chiudono alcune brevi notazioni.

## *2. Di quale guerra parliamo?*

Ci hanno attaccati e siamo in guerra, ma è difficile capire di quale guerra si tratti.

Negli ultimi decenni questa guerra è sempre continuata, secondo un andamento "carsico", in teatri e con intensità diversi; quindi, non esiste una vera e propria soluzione di continuità tra queste ondate di forte recrudescenza del terrorismo islamico; a volte le sue sembianze sono la sintesi delle mutate condizioni di contesto sia nel versante del nostro nemico, sia nel versante dell'aggredito, occidentale e non. Alcuni aspetti sono comuni a quelli della prima generazione di *jihād*; altri appaiono con accenti e in toni diversi; altri sono inediti, peculiari dell'attuale guerra.

### *2.1. Un prisma dalle molte sfaccettature*

Sono guerre civili, alcune delle quali ci tornano indietro come *boomerang*: la Libia del dopo-Gheddafi, implosa in vecchie lotte tribali e sprofondata nel caos pieno; l'Iraq del dopo-Saddam, con profughi e sfollati, attentati e violenze; il Libano (la cui religione, per il solo filone

musulmano, si articola principalmente in sunnita, sciita, ismailita), minacciato dallo scontro interno fra religioni.

Inoltre, ai conflitti interni si sovrappongono le guerre fra Stati (o sedicenti tali) per l'egemonia regionale: Arabia Saudita, Turchia (accomunate dall'opposizione al regime siriano), Egitto, Iran. La guerra fra Iran e Arabia Saudita – che le sembianze di una guerra di religione coprono quella vera per le risorse energetiche – trascina con sé molti altri paesi: Siria, Yemen, Libano, Afghanistan, Pakistan, Bahrain.

Si aggiungono i conflitti tra gruppi terroristi[2]. La verità è che l'*Ummah*, la comunità dei credenti islamici, è in guerra con se stessa, agevolando il proliferare di tali gruppi.

Tali stratificazioni si accrescono con l'intervento della comunità internazionale: la coalizione, costituita da circa 60 paesi e capeggiata dagli Stati Uniti, che per primi (2014) hanno iniziato i bombardamenti in Iraq. Nascono inedite alleanze e a geometria variabile, prima fra tutte quella fra Stati Uniti e Russia. E intrecci e legami tra Stati Uniti e gruppi terroristi[3].

Prolifera il dibattito se sia possibile contrastare l'Is senza ricorrere alle armi.

---

[2] La rivalità più nota è quella tra i Fratelli Musulmani, sostenuti dal Qatar, e i Salafiti sostenuti dall'Arabia Saudita in Egitto, in Libia e in Tunisia. Più di recente, l'Is combatte per la supremazia della *jihād* "globale" contro il Fronte al Nusra, che rappresenta in Siria al-Qaeda, ormai fortemente indebolita. Ma anche all'interno del Fronte al Nusra ci sarebbe una scissione tra i conservatori, fermamente intenzionati a mantenere legami con al-Qaeda, e un gruppo sostenitore di un nuovo approccio incentrato esclusivamente sul problema siriano. Inoltre, sembrerebbe che Turchia, Arabia Saudita e Qatar stiano rafforzando Ahrar al-Sham (un gruppo armato siriano, che durante la guerra civile in Siria cercò di abbattere il governo di Assad, giudicato autoritario), nel tentativo che la crescita di tale organizzazione rivale metta in difficoltà al Nuṣra e la spinga a separarsi da al-Qaeda per cercare nuove alleanze. Nel 2014, i ribelli affiliati al Fronte Islamico e l'Esercito Siriano Libero lanciarono un'offensiva in Siria contro i combattenti di Isad Aleppo. Si veda, H. SAAD, R. GLADSTONE, *Qaeda-Linked Insurgents Clash With Other Rebels in Syria, as Schism Grows*, in *The New York Times*, 04.01.2014.

[3] È stato ripreso attraverso fotografie e video un senatore statunitense, John McCain, in compagnia di rappresentanti di fazioni opposte al regime siriano, fra cui al-Baghdadi. In alcune interviste televisive mandate in onda da *Fox* e *CNN*, egli ha rivelato il supporto a gruppi ribelli in funzione anti-Assad in Siria.

Attentati e guerre, se ormai diventate una triste *routine* nei paesi a sud del Mar Mediterraneo – soprattutto nei teatri mediorientali –, costituiscono eventi ancora eccezionali nei paesi occidentali.

Diventa inevitabilmente uno scontro fra civiltà. Con *Westoxication* gli islamisti radicali indicano gli effetti esiziali della cultura occidentale su quella del mondo islamico[4].

Gli aggressori colpiscono nel profondo, fino alle Istituzioni nazionali e a quelle della UE; destrutturando la normalità dei paesi attaccati, dove tutti si sentono potenziali bersagli; mettendo in discussione persino il diritto internazionale sull'obbligo di accoglimento dei profughi in fuga dalla violenza e dalle guerre. A ricaduta, pregiudicando l'*aquis* di Shengen e la "rotta balcanica".

È evidente, dunque, come il terrorismo transnazionale presenti fattori di complessità maggiori di quello interno, in quanto il primo è generalmente connesso a un profondo *gap* fra dotazioni di ambiente, cultura, religione, aspetti socio-economici, tra cui le scale valoriali: sono due esempi, il valore della vita stessa da parte di chi sacrifica la propria per la causa, nonché la divergenza abissale nell'interpretazione dell'atto violento, secondo la diade "terrorismo-gesto eroico".

È anche una guerra di religione o, quantomeno, spacciata come tale dai "burattinai": le *élite* e i *coach* della fidelizzazione. Nei *failed States*, o in quelli con bassi livelli di *governance*, l'elemento religioso costituisce un importante input politico. Basti pensare a come sia l'*ayatollah* Khomeini e Saddam Hussein sia il califfo rispettivamente si rappresentassero e si rappresenti discendenti di Maometto. Il terrorismo religioso, proprio per la sua portata messianica, nichilista ed olistica, per la sua valenza politica, è forse il più pericoloso.

Inoltre, l'area geopolitica dell'aggressore fruisce di un elevato valore aggiunto: considerate comunemente arcaiche, le forme sociali prevalenti nel mondo islamico sono capaci di creare un elevato stock di capitale sociale (a basso costo). Rapporti tribali e clanici, fedeltà, legami di fiducia, rispetto per le proprie radici, senso di appartenenza alla comunità, creano una massa critica all'interno dell'azione collettiva contro l'Occidente.

[4] R. GUOLO, *L'ultima utopia. Gli jihadisti europei*, Milano, 2015.

Già Adam Smith aveva messo in risalto la rilevanza, all'interno di una società, di valori quali il senso del bene comune, l'influenza dell'identità sociale sul comportamento[5], vale a dire l'importanza di una dotazione di "beni relazionali", secondo l'attuale terminologia economica.

Fra le parti in conflitto, si contrappongono l'individualismo e il senso di sradicamento e, ancora, la noia tutta *bohémien* di chi "nasce bene" e trova nel radicalismo(chic) – qualunque esso sia – un placebo esistenziale; e, poi, *banlieues* povere, criminalità, derive. E, ancor più inquietante, il rifiuto nei confronti dell'Alterità e di tutto quel che ne segue ineludibilmente… Oliver Roy ha pubblicato un lungo editoriale su *Le Monde*[6], affermando che non staremmo sperimentando la "radicalizzazione islamica della società", bensì l'"islamizzazione della radicalizzazione sociale". Non sarebbe, quindi, l'ideologia islamica che induce le persone a radicalizzarsi. La radicalizzazione è un processo già in atto e attuato per tappe successive; per taluni, essa assumerebbe i simboli dell'islamismo radicale.

Quando si combinano i fattori religioso, politico e sociale, contribuendo all'idea del sacrificio della propria vita come quello del vero "eroe" o, in chiave darwiniana, come il gesto per la continuità della propria specie, allora la lotta fra i due schieramenti diventa ìmpari.

Questa guerra ha creato casi parossistici. Il primo, fra tanti, fa riferimento all'attentato terroristico perpetrato da al-Qaeda contro la sede di Charlie Hebdo, avvenuto nel gennaio 2015, dove sono state uccise dodici persone, tra cui un poliziotto musulmano, Ahmed Merabet, per mano di *foreign fighter*, falsi musulmani. È una guerra dove, in questo groviglio confuso e poliforme, le vittime vengono uccise persino dal "fuoco amico", o, meglio, da falsi amici.

Il secondo paradosso è che oggi l'Europa si configura in una diade, allo stesso momento obiettivo e roccaforte[7], dove i terroristi si autoreclutano (soprattutto tramite il *dark/deep web*), cercando – nelle co-

[5] A.K. SEN, *La ricchezza della ragione. Denaro, valori, identità*, Bologna, 2000.

[6] O. ROY, *Le djihadisme est une révolte nihiliste*, in *Le Monde*, 25.11.2015.

[7] M. FIOCCA, G. MONTEDORO, *Diritto alla sicurezza ed economia del terrore*, Roma, 2006.

munità che vanno così formando – una nuova identità, sostitutiva di quella musulmana scemata nel corso delle generazioni.

Nel riconoscimento reciproco, in Europa il terrorismo *jihādista* può fare da collante ed essere interpretato come un movimento di liberazione nazionale o guerra civile ed etnica, come nel caso dell'IRA o dell'ETA o di quello ceceno.

Questa è anche una *proxy war*, una guerra combattuta per interposta criminalità autoctona.

È una guerra economico-finanziaria. Il finanziamento – in particolare, una rete sicura di fonti – è la linfa per tali organizzazioni. La costruzione di una propria rete di finanziamento è stata uno degli obiettivi primari di bin Laden affinché la sua organizzazione potesse contare su una solida base di milioni di dollari. In quella generazione, ciascun atto terroristico non ha richiesto somme particolarmente ingenti e, pur essendoci un forte divario di costi fra l'attacco di New York e quello di Londra, entrambi hanno avuto successo.

Proprio per questo, limitarsi a studiare tali fenomeni attraverso la geopolitica è uno sforzo monco, che forse trascura gli elementi che muovono tutto: l'economia e la finanza.

Infatti, studiosi di frontiera affermano come il campo militare sia sempre meno decisivo nel condizionare gli esiti di un conflitto. Altri fattori, primo fra tutti quello economico-finanziario, risultano invece sempre più determinanti. L'Is è un decisivo banco di prova di queste teorie.

Sempre sul piano della finanza, il saccheggio – il bottino di guerra – da parte del nostro nemico ha delle proprie peculiarità: l'"islamizzazione degli *asset* occidentali", già realizzata nella generazione 1.0. Il progressivo sfruttamento ad opera del terrorismo degli *asset* occidentali si estende alle pratiche di *insider trading*, a quelle di aggiotaggio, alle speculazioni di Borsa e a scelte di portafoglio ben congegnate. Ad esempio, a pochi giorni dall'attentato dell'11/9, erano stati operati acquisti molto elevati di Buoni del Tesoro statunitensi a scadenza quinquennale: investimento ideale in un clima di incertezza, in cui i titoli azionari subiscono forti perdite in conto capitale; in altri termini, una scelta ottimale in periodi di *fear economy*.

Anche l'"occidentalizzazione" degli *asset* islamici, con la grande diffusione di fondi di investimento islamici regolamentati dal Comitato della *sharia*, possono presentare notevoli vantaggi per il terrorismo: costituiscono una tecnica per "lavorare" il suo denaro, nella duplice direzione di *money laundering* e *money dirtying*.

L'esportazione in Occidente della finanza islamica avviene tramite sia la finanza etica sia attraverso operazioni di ingegneria finanziaria volte ad eludere il divieto di remunerare i prestiti.

Anche questa guerra si avvale quindi diffusamente della corruzione (cfr. par 1.2) e della criminalità. Ciò in una duplice direzione: il criminale diventa terrorista (per "rifarsi una verginità" surrogata da ideali più elevati); il terrorista diventa criminale (per autofinanziarsi e, quindi, scendendo a patti con la prosaicità del quotidiano). Un Rapporto dell'OCSE[8] stima, ad esempio, che il contrabbando di sigarette abbia prodotto una perdita di gettito agli Stati pari circa a 40 miliardi di dollari nel 2010: ma, soprattutto, che esso sia andato a finanziare *jihādisti* in Medio Oriente.

Il Cremlino ha ricevuto "recentemente" nuovi rapporti d'*intelligence* che documenterebbero un traffico di petrolio dai territori controllati dall'Is alla Turchia "su scala industriale". Se la Turchia protegge gli *jihādisti* dello Stato islamico, ci sono petromonarchie del Golfo, quali l'Arabia Saudita e il Qatar, che li finanziano[9].

Secondo la FATF (*Financial Action Task Force*), la maggioranza dei governi non solo non si impegna realmente nella lotta contro gli stretti legami tra la finanza internazionale e le reti del terrore, ma, al contrario, è compiacente. Un caso rilevante è proprio quello dell'Arabia Saudita, che "usa gli standard del Fatf per difendersi in casa sua" (*not in my backyard*!), ma "li viola totalmente nelle sue attività estere e internazionali". Infatti, il paese, se da un lato detiene il primato delle azioni contro i reati che collegano finanza e terrorismo, dall'altro è, con il Qatar, il più grande finanziatore e sostenitore degli *jihādisti*.

[8] OCSE, *Illicit Trade. Converging Criminal Networks*, Parigi, 2016.

[9] N. PARKER, L. IRELAND, *Iraqi PM Maliki says Saudi, Qatar openly funding violence in Anbar*, in *Reuters*, 09.03.2014; N. BOZORGMEHR, S. KERR, *Iran-Saudi proxy war heats up as Isis entrenches in Iraq*, in *Financial Times*, 25.06.2014.

Nell'audizione dedicata al *Terrorism Financing and the Islamic State*, organizzata nel novembre 2014 dalla Commissione per i Servizi finanziari del Congresso americano, è emerso con chiarezza che

> mentre al Qaeda poteva contare dopo l'attentato dell'11/9 su circa mezzo milione di dollari di sostegni al giorno, l'Isis aveva introiti di 1-2 milioni di dollari al giorno attraverso la vendita di petrolio, i riscatti degli ostaggi e i sostegni da parte delle organizzazioni caritatevoli soprattutto dei Paesi del Golfo, a cominciare dal Qatar e dall'Arabia Saudita.

Nel commercio del petrolio, il partner principale dei terroristi dello Stato islamico è sicuramente la Turchia.

> Circa 30mila barili al giorno, trasportati da 250 autobotti transitano attraverso i confini porosi della Turchia e del Nord Iraq per essere venduti a compiacenti acquirenti, consapevoli di sostenere le operazioni terroristiche.

Al petrolio, si aggiunge il gas.

Inoltre, la guerra dell'Is si svolge su teatri territorialmente diversi, distanti e simultanei: nei paesi del Golfo, e, in particolare in Kuwait (colpito il 26 giugno 2015), e in Arabia Saudita (più volte nel maggio 2015), ma anche in Tunisia (il 18 marzo presso il Museo del Bardo e il 26 giugno 2015, stesso giorno di Kuwait City, presso una località turistica) e in Turchia (il 20 luglio successivo). La lista non è esaustiva.

È una guerra in continua *escalation*, "colpo su colpo".

È una guerra-guerriglia, che sconvolge quartieri e coinvolge civili.

È la terza guerra mondiale[10]? Se la Guerra Fredda è stato l'ultimo tentativo di gestire un ordine mondiale basato sulla deterrenza reciproca fra i due blocchi, l'attuale realtà è invece "liquida", mutuando l'espressione di Bauman[11], dove la guerra filtra ovunque fra i gangli aperti dell'Occidente; inonda le fondamenta delle istituzioni dell'Unione europea; scorre fra i delicati rapporti dei primattori mondiali Stati Uniti-Russia-Cina; si insinua fra le vaste plaghe prive di *governance*; penetra

[10] Per un'ampia visione di quadro, L. CARACCIOLO, *Non è la fine del mondo*, in *Limes*, n. 2, 2016.

[11] Z. BAUMAN, *Modernità liquida*, Bari, 2011.

nel caos sistemico mediorientale; sfrutta gli interstizi della lotta fra gli avidi Stati del Golfo, in particolare fra i grandi rivali Iran e Arabia Saudita. È una guerra liquida come il petrolio – il cui corso ha destabilizzato l'economia mondiale –, è anche una guerra (di prezzi) fra tipologie di petrolio, in particolare contro l'olio scisto statunitense[12]. Come falde freatiche, la guerra ritorna in superficie creando shock sistemici nei vari settori dell'economia (reale, finanziario, valutario), con una intensità più o meno violenta a seconda della "porosità" dei fondamentali stessi. Come nello scioglimento dei ghiacciai, le slavine che si staccano colpiscono al pari di razzi e proiettili impazziti. Come l'alta marea, la guerra lascia sulla spiaggia corpi(cini) morti e detriti. Come in un naufragio, arrivano le zattere dei superstiti approdando in luoghi loro sconosciuti se non nelle mappe. Come la rottura di una diga, la guerra copre territori, abitazioni, luoghi sacri, *suq*, falcidia la popolazione. Come flutti, essa immerge e porta lontano i nostri *asset*, persino quelli immateriali quali i sofisticati *know-how* del *cyber* e le strategie mediali di avanguardia. Goccia dopo goccia, forma stalattiti e stalagmiti di odio che si cristallizza e si consolida.

Quanto distanti i precedenti eventi bellici mondiali "convenzionali"! Mancavano della "liquidità e "sinuosità" di un rettile che si infiltra e colpisce mortalmente. Al contrario, c'erano simmetria fra le fila nemiche, compattezza degli schieramenti avversari, ordine, disciplina. Regole di un tempo che fu.

Una guerra dai mille rivoli, quella attuale.

E se questa è una guerra liquida, dove ci farà approdare?

### *2.2. Terrorismo e corruzione*

*Transparency International* definisce corruzione come "l'abuso di pubblici uffici per il guadagno privato". La corruzione ambientale, o endemica, si verifica quando la corruzione non è un atto isolato, ma comune e quasi consuetudinario.

[12] Si tratta del nuovo combustibile fossile, di cui gli USA sono diventati importanti esportatori.

In un recente documento[13], l'OCSE argomenta come corruzione e terrorismo si rafforzino reciprocamente nei paesi in guerra, dove le attività criminali prosperano. Criminalità e terrorismo usano la medesima area grigia – corrompendola – dei sistemi legali, nonché la porosità dei sistemi finanziari per canalizzare le proprie fonti di finanziamento. Sintetizzando i principali aspetti: a) i paesi, indeboliti da una corruzione endemica, hanno maggiori difficoltà nel combattere il terrorismo; b) la corruzione nel settore della difesa – tipicamente colpito dalla corruzione, soprattutto ad opera dei lavoratori nei paesi dove l'industria delle armi è forte, molti dei quali dell'area OCSE – pregiudica la sua efficienza, nonché la capacità di far fronte a gruppi quali l'Is o Boko Hara. I militari sono mal pagati e mal equipaggiati, e basso il loro morale, poiché le risorse a loro destinate vengono convogliate nelle commissioni per l'approvvigionamento. Malgrado l'emanazione di normative anti-corruzione nella maggior parte dei paesi, uno studio del 2015 di *Transparency International* documenta che 2/3 (pari a 107) delle società che operano nel settore della difesa sono scarsamente attrezzate per contrastare la corruzione; c) in ambito giudiziario, molti magistrati e legali vengono corrotti dalla criminalità e dal terrorismo, che riescono così a creare un network che ostacoli le indagini o che faccia evitare loro la detenzione preventiva; d) la corruzione è la "tecnologia", che mette in grado molti terroristi di effettuare atti criminali. Per esempio, due dei terroristi dell'11/9, ottennero patenti di guida illegali rilasciate dalla *Virginia's Division Motor Vehicles*, che vennero utilizzati come documento di riconoscimento per imbarcarsi sull'aereo; e) i terroristi sono spesso in grado di corrompere il personale negli aeroporti per far passare attraverso i sistemi di sicurezza armi e bombe; f) molti esperti sostengono che la corruzione aumenti il rischio che i terroristi si impadroniscano di materiale nucleare. Il maggiore pericolo oggi è la connessione tra gli addetti corrotti che hanno accesso al materiale nucleare, i gruppi criminali che già ne controllano il transito, i terroristi che lo acquistano. Questo snodo è tra i più rischiosi per la stabilità internazionale di oggi.

[13] OCSE, *Terrorism, corruption and the criminal exploitation of natural resources*, Parigi, 2016. Si veda anche L. SHELLEY, *Dirty entanglements: Corruption, crime and terrorism*, Cambridge, 2014.

Non c'è ancora una diffusa consapevolezza dell'esistenza di tale triade e come essa si rafforzi reciprocamente. Nel 2014 e nel 2015, varie Risoluzioni del Consiglio di Sicurezza delle Nazioni Unite (2253, 2199 rispettivamente del dicembre e di febbraio 2015; 2195 del dicembre 2014) hanno riconosciuto che i gruppi terroristi funzionano come gli affaristi nel campo delle attività criminali internazionali. Stessi strumenti, obiettivi diversi, come ampiamente analizzato dalla FATF (cfr. par. 5). La circostanza sempre più evidente, commenta l'OCSE, è che il terrorismo si annida nelle aree di attività particolarmente vulnerabili alla corruzione. Essa si svolge in snodi di confine, dove la criminalità può corrompere il personale alla dogana così da vendere beni vietati. Fra armi, antichità, persone, l'affare più lucrativo per l'Is, commenta l'OCSE, è il contrabbando di petrolio.

Tra i principali canali di veicolo, le *shell companies*, definite dall'OCSE come "a company that is formally registered, incorporated, or otherwise legally organised in an economy but which does not conduct any operations in that economy other than in a pass-through capacity". L'unico scopo è nascondere l'identità del vero proprietario dei soldi, o, più genericamente, il *beneficial ownership*, secondo la terminologia delle autorità fiscali e degli altri organismi che combattono l'evasione e le attività finanziarie illegali.

Come affermato in numerosi documenti della Banca d'Italia, le transazioni avvengono diffusamente attraverso le valute virtuali[14].

### *2.3. Non c'è guerra senza economia (e non c'è economia senza guerra)*

A complicare la governabilità sistemica è l'evoluzione dell'economia mondiale, che dà il polso del clima di fiducia. All'idea della crescita illimitata (ormai riposta in soffitta), si contrappone l'altrettanto irrealismo dell'economia della felicità e della bontà della decrescita, forme

[14] Un attuale approfondimento tecnico è in M. FIOCCA et al., *La jihād 2.0: profili economici, tecnologici, giuridici*, in *Ciberspazio e Diritto*, n. 1, 2016. In particolare, il par. 6 sulle nuove frontiere tecnologiche del cyberterrorismo e sulle valute virtuali. Sulla parte diritto e terrorismo, in particolare per gli strumenti di contrasto e sul "captatore/*trojan* di Stato", si rinvia al par. 7.

di *divertissement* intellettuali e coreografiche, che oggi si rivelano in tutta la loro pateticità.

Nella UE, il diffuso euroscetticismo si accompagna a forze centrifughe, invertendo il processo di integrazione e favorendo l'ordine sparso.

Al suo interno, il Belgio è considerato l'anello debole nella lotta europea contro l'estremismo, per diversi motivi e, soprattutto: *1)* è fallita l'integrazione politica tra fiamminghi e valloni; *2)* le due comunità discriminano l'identità in ufficio, a scuola, all'università. Ne scaturisce l'esclusione e l'emarginazione sociale, a maggior ragione nei confronti dell'immigrato, che non si sente neppure belga. E, infatti, in Belgio vive una consistente e poco integrata comunità musulmana e, all'interno di questa, un'elevata disoccupazione giovanile; *3)* l'emarginazione sociale può portare all'estremismo religioso, dove il soggetto trova identità e ragione di essere. Infatti, in Belgio esiste un gran numero di *foreign fighters*; *4)* un paese spaccato è un paese debole, è un paese dove è estremamente difficile formare una compagine governativa (il Belgio ne è stato privo per oltre un anno), è un bersaglio relativamente facile per il terrorismo; *5)* i risparmi di spesa nelle politiche per la sicurezza sono stati eccessivi; *6)* come negli USA, il paese ha una lunga storia di leggi permissive sulle armi ed industrie che producono armi. La maggior parte degli attacchi perpetrati in Europa negli ultimi tempi ha legami con il mercato belga, di cui – è stato affermato – il 90% delle armi proviene dai Balcani.

In Europa, il succedersi delle crisi – finanziaria (2008), economica (2009), dei debiti sovrani (2010) – ha dato conto della necessità della revisione delle regole della nuova *governance* economica, che ha inasprito i rapporti fra Stati membri e provocato una diffusa insofferenza verso le regole numeriche, alcune delle quali hanno effetto prociclico. Anche la massa dei profughi pesa sui conti pubblici, acuendo ulteriormente le tensioni all'interno e fra Stati membri. E poi, il connubio recessione-deflazione. Quest'ultima viene esacerbata dallo shock petrolifero, originato dalla guerra dei prezzi del greggio, che vuole portare il *competitor* allo sfinimento, ma che tuttavia non può durare ancora molto a lungo per la sopravvivenza delle stesse parti contendenti, soprattutto ora, senza più un cartello. Inoltre, la deflazione rende insostenibile i

parametri fiscali europei, uno fra tutti la dinamica del rapporto fra debito pubblico e Pil.

Per contrastare l'esiziale diade recessione-deflazione e stimolare la domanda aggregata anche tramite un clima di fiducia più disteso, le Banche Centrali delle due sponde dell'Atlantico hanno effettuato manovre espansive, volte ad abbassare il tasso di interesse: così per la BCE, con il *quantitative easing* e il *forward guidance*. Ma la riduzione dei rendimenti produce indesiderati effetti collaterali: reputazionali nei confronti delle istituzioni da parte dei risparmiatori-investitori; redistributivi a favore del debitore (le istituzioni); la ricerca da parte del risparmiatore di *asset* più remunerativi, che di conseguenza accrescono la rischiosità e la fragilità sistemica.

Il passaggio di bolla in bolla, gli attacchi speculativi, le maglie larghe e opache della regolamentazione, rendono il settore finanziario particolarmente vulnerabile, malgrado i progressi nella sua resilienza. Ed è noto come il sistema finanziario e quello valutario assolvano un importante ruolo nell'ordine internazionale. A riprova, le tensioni create dal tasso di cambio fra yuan cinese e dollaro, a seguito delle successive svalutazioni del primo, che benché non nate come svalutazioni competitive, di fatto portano allo stesso risultato. E le lezioni apprese dalla storia (*beggar-thy-neighbor*) ci ricordano la loro portata conflittuale.

Ritornando all'economia reale, il commercio deve essere interpretato nel suo duplice ruolo: causa di guerra (non c'è economia senza guerra) e vittima di guerra (non c'è guerra senza economia). Il risultato è comune: il suo rallentamento, con le inevitabili ricadute sulla crescita. Sul primo aspetto, ad inasprire i rapporti: *dumping* di varia natura, discriminazioni commerciali (quali le aree di libero scambio), contingentamenti, cartelli internazionali, misure surrettiziamente protezionistiche (quali le barriere tecniche al commercio - TPB), il protezionismo da regolamentazione, ecc.; inoltre, embarghi e conseguenti ritorsioni, cui si è fatto ricorso anche in questa guerra contro lo *jihāddismo*. Sul secondo aspetto, le ricadute sull'economia: le misure di sicurezza, che incidono sui tempi per i controlli e coincidono con la chiusura dei confini. Due esempi al riguardo: all'indomani dell'11/9, quando i confini sono stati temporaneamente chiusi, gli autotrasportatori tra USA e Canada hanno dovuto attendere fino a 20 ore per una traversata che nor-

malmente richiede qualche minuto. All'indomani dell'attentato alla sede di Charlie Hebdo, il governo francese ha comunicato le sue intenzioni di ridimensionare gli scambi commerciali con i paesi simpatizzanti culturalmente e religiosamente con le organizzazioni terroristiche ritenute responsabili degli attacchi.

Inoltre beni, che la teoria economica tradizionalmente non considerava economici – in quanto non connotati dalla "scarsità" –, diventano oggetto di guerre. Guerre per la conquista di risorse naturali: acqua e terra, a seguito dei processi di desertificazione, ecc.

Ancora sul piano della distribuzione delle risorse a fondamento del conflitto – compreso quello *jihāddista* –, vi è la disuguaglianza. La frustrazione da *gender*, ormai si fonda su una interdisciplinarietà molto ampia e consolidata.

Già Keynes, e molto dopo alcuni filoni interdisciplinari fra economia e psicologia (fra gli autori più noti, Kahneman-Tversky), sottolineano come non sia la condizione economica assoluta a creare il conflitto, bensì il confronto fra le posizioni relative. Il conflitto non sorgerebbe se tutti vivessero nelle *banlieues* degradate, ma nasce dal confronto tra chi vive a Parigi nelle *banlieues* più misere e chi nel XVI quartiere. Tali privazioni relative costituiscono, nell'approccio di Sen, *incapacitazioni* a raggiungere lo stesso funzionamento sociale di altri nell'ambito della medesima comunità, circostanza questa che rafforza l'esclusione.

Proseguendo il filone di ragionamento di Sen, è dirimente l'ulteriore distinzione fra disuguaglianza economica e disuguaglianza di reddito. L'enfasi posta sul secondo indicatore nel valutare la disuguaglianza, come tradizionalmente avviene, crea un quadro distorto, che porta a trascurare *privazioni* legate ad altre variabili, come la cattiva salute, la mancanza d'istruzione, l'esclusione sociale e, sul solco rawlsiano, la "capacitazione" di *scegliersi una vita cui si dia valore* e che *dia il rispetto di sé*[15]. E questi sono indubbiamente importanti argomenti che contribuiscono ad interpretare il successo del proselitismo.

In una società globalizzata, la comparazione e la capacitazione relativa si fondano non solo all'interno di una determinata società, ma fra

[15] A.K. SEN, *Lo sviluppo è libertà*, Milano, 2000.

società[16]. Tali argomenti, insieme a quelli di Runciman[17], sono modi di leggere l'odio verso l'Altro, verso chi ha capacitazione e possibilità di scegliere la propria vita e che è messo in grado di avere rispetto di sé. E questi sono indubbiamente importanti argomenti che contribuiscono ad interpretare il successo dello *jihāddismo*.

La prospettiva sociologica di Runciman mette in rilievo la differenza fondamentale tra la frustrazione generata da un'ingiustizia vissuta solo a livello individuale e una invece perpetrata a livello collettivo. La prima condurrebbe a fenomeni di devianza individuale – la piccola criminalità, ad esempio –; la seconda sarebbe associata ad azioni collettive, come la partecipazione a movimenti di protesta, fino ad arrivare al terrorismo.

La deprivazione relativa sul piano collettivo è indotta da quella individuale: un soggetto che giudica iniqua la propria posizione potrebbe essere indotto a non farne un caso meramente personale, bensì un atteggiamento generale rivolto al suo gruppo di appartenenza. Tale passaggio dall'"individuale al collettivo", se è di immediata comprensione nel caso della razza o della religione, in altri casi è più complicato. Un soggetto potrebbe sentirsi membro di un gruppo "oppresso" da un "oppressore" (tipicamente nella lotta fra la classe operaia e la proprietà; i musulmani oppressi da un Occidente colonialista e apostata; un cittadino appartenente ad un paese la cui *élite* gode di privilegi ed è governato da una classe politica collusa e corrotta).

Fra tanti tipi di oppressioni disponibili sul "mercato dell'ingiustizia", l'oppresso può scegliere un proprio "paniere" sulla base della scala delle sue preferenze: un proletario potrebbe essere musulmano, ma preferisce privilegiare (e lottare per) la sua identità di classe operaia, anziché entrare nelle fila della propria confessione religiosa. In tale scelta, egli/ella potrebbe essere guidato/a, ad esempio, da un metodo di "ancoraggio", ovvero seguire le scelte compiute già da altri soggetti percepiti come simili (*herd behaviour*) o, ancora, tramite il plagio e la manipolazione. Queste scelte, benché abbiano lo stesso tipo di radica-

[16] A.K. SEN, *op. cit.*

[17] W.G. RUNCIMAN, *Sociology in Its Place and Other Essays*, Cambridge, 1970.

lizzazione sociale, portano a risultati profondamente diversi, fino ad arrivare all'uso della violenza, scelta che diventa strutturale nella *jihād*.

Il professore iraniano di psicologia, Mogahaddam[18], ha spiegato, tramite la metafora della "scala" (*Staircase model*), il processo di radicalizzazione che culmina con l'uso della violenza. Sul primo gradino si posizionano tutti coloro che si sentono variamente vittime di ingiustizia e di *gender*, mentre in vetta arrivano quei (relativamente) pochi che, per combattere l'ingiustizia, indirizzano l'uso della violenza verso coloro ritenuti responsabili di tale ingiustizia, ad esempio l'Occidente.

I sostegni immediati per raggiungere l'ultimo gradino sono la crisi economica e la disuguaglianza. Che vi arrivino ragazzi, istruiti e *outsider* sul mercato del lavoro appare alquanto scontato.

Sottostanti ad ogni guerra lavorano quindi tante e diverse spinte economiche, dandone anche la direzione, se non gli esiti. Nel quadro attuale, tale gioco di spinte e contro-spinte si rafforzano. Dunque, ci troviamo in un contesto sistemico funambulesco… dove lo *jihāddismo* sguazza, si mimetizza e amplia i propri spazi.

### *3. L'innovatività della* jihād *di seconda generazione*

Nello Stato Islamico[19], molti osservatori occidentali ritrovano in al-Qaeda un'organizzazione anacronistica che vuole riportare indietro le lancette dell'orologio. Rifugiati siriani e iracheni confermano questa tesi.

Ma ciò è confutabile – come pensare che il movimento statunitense di matrice liberale, il *TEA* (*Tax Enough Already*) *Party*, pretenda di tornare al 1773 (con la protesta dei coloni del Nord America contro le tasse inglesi) – poiché sembra una semplificazione riduttiva: mentre il

[18] F. MOGAHADDAM, *The Staircase to Terrorism: A Psychological Exploration*, in *American Psychologist*, 2005.

[19] Esso è l'icona della seconda generazione dell'islamismo radicale, cui è garantito supporto dai filippini di Abū Sayyāf, dagli algerini del Battaglione al-Hudā, dai Mujāhidīn dello Yemen, dai pakistani di Tehrik-e-Khilafat, dai nigeriani di Boko Haram, dai sudanesi della Devozione al Corano e dalla Sunna. L. CARACCIOLO, *Ultime dalla Terra di Hobbes*, in *Limes*, n. 9, 2015.

mondo dei talebani era sostanzialmente circoscritto alle scuole coraniche, il brodo di coltura dello Stato Islamico è pragmatismo e modernità.

Sul piano più pragmatico, gode di importanti *asset* rispetto ad al-Qaeda.

Ha addirittura elaborato un Manuale (sebbene se ne dubiti l'autenticità), pubblicato in esclusiva dal quotidiano *The Guardian*: *The Isis papers: a masterplan for consolidating power*[20], per la costituzione di un Califfato efficientemente organizzato in dipartimenti civili e militari.

Tranne debite importanti eccezioni (quali il Qatar e l'Arabia Saudita), non si avvale di Stati sponsor, le cui fonti di finanziamento sono vulnerabili e aleatorie. È autosufficiente e si è privatizzato (con la c.d. *Reaganomics* del terrore), utilizzando il proprio denaro per impiantarsi in snodi strategici, come le ricche aree petrolifere della Siria orientale.

In più, a differenza di al-Qaeda, ha un proprio – e ampio – territorio, anzi di più, un sedicente Stato (delle dimensioni circa del Regno Unito, con 6 milioni di abitanti).

Ha una sua banca centrale e batte moneta avendo annunciato, nel novembre 2014, di coniare una propria valuta con corso legale in tutti i territori controllati dall'Is (il "dinaro d'oro", ma esiste anche in argento e rame), in competizione con il dollaro, come il Califfato millanta (benché, ad ogni buon conto, gli stipendi vengano pagati in dollari), con un proprio tasso di cambio e, secondo l'economista iracheno Basim Jameel, prodotto con macchinari italiani importati in Iraq.

Il conio di una divisa d'oro, dove l'oro è il tradizionale bene-rifugio, è molto significativo. La sua adozione da parte di gruppi come Is è volta ad agganciarsi a un bene universalmente riconosciuto e sufficientemente stabile nel prezzo. Un'àncora di salvataggio da parte di chi, in effetti, può morire delle oscillazioni del settore finanziario non avendo dietro la protezione legale di uno Stato, né tantomeno di una comunità internazionale e delle IFI che si adoperino per il salvataggio.

Ha un apparato amministrativo molto articolato[21], un esercito regolare e un comando militare efficace e disciplinato, che spostano l'azione

[20] 10.03.2016.

[21] Esso è strutturato in un Consiglio di Sicurezza, in un Consiglio militare, un Consiglio della Sharia, un Consiglio della Šura, un Consiglio dei Media, un Dipartimento

dove individuano i gangli più deboli, con attacchi a sorpresa e ad elevata produttività. Attacchi basati su manovre fluide, come «il movimento di un serpente fra le rocce»[22].

La *leadership* dell'Is è costituita prevalentemente dall'*intelligence* irachena e da uomini del regime di Saddam, estromessi dopo l'invasione USA del 2003, molto ben formati, che hanno importato nell'Is capacità militari, obiettivi politici mutuati dal Partito baathista, informati sui percorsi dei traffici illegali di petrolio e beni, sviluppati nel corso degli anni 90 dal regime iracheno per eludere le sanzioni internazionali[23]. Inoltre, l'Is si serve anche dei tecnici di Saddam esperti dei sistemi idrici del Tigri per condurre la guerra dell'acqua, da quando, con i bombardamenti USA, l'Is ha perso la grande diga di Mosul in Iraq. I miliziani conquistano le dighe e chiudono i rubinetti per costringere le popolazioni a lasciare il territorio.

Da qui un'ulteriore importante differenza fra le due generazioni: mentre la *jihād* 1.0, in particolare al Zarqawi, fece l'errore di marginalizzare gli ex funzionari iracheni, la *jihād* 2.0 crede nel loro innesto come forma di valore aggiunto al proprio progetto[24].

---

delle Finanze, una Organizzazione amministrativa per la riorganizzazione del territorio in province. Si veda L. CARACCIOLO, *Non è la fine del mondo*, cit.

[22] L. NARBONE, *Lo Stato Islamico: il jihād e la paura*, in AA.VV., *Contro la paura*, Milano, 2016.

[23] È stato scritto (J. STERN, J.M. BERGER, *Isis: Inside the Army of Terror*, New York) che l'ascesa dell'Is è sostanzialmente parallela alla storia dell'Iraq, quali la crudeltà del regime baathista e sunnita di Hussein, lo smantellamento dell'esercito iracheno, la conseguente guerriglia e la marginalizzazione degli iracheni sunniti da parte del governo dominato dagli sciiti, la legge per "debaathizzare" l'Iraq (sempre ad opera statunitense), sulla cui base 400mila uomini dell'esercito iracheno furono esclusi da incarichi militari, fu negata loro la pensione, ma venne concesso loro di tenere le armi. Comune al regime iracheno e all'Is è la perpetrazione della crudeltà verso la popolazione per la sua sottomissione. Alcune scene di violenza e di addestramento dell'epoca di Hussein assomigliano significativamente a quelle diffuse dall'Is. Inoltre, sia il regime iracheno nel passato sia l'Is oggi si autopercepiva e autopercepisce rispettivamente come movimento transnazionale, che giustifica(va), tra l'altro, la formazione di campi di addestramento diffusi in Medio Oriente.

[24] È oggetto di dibattito perché molti iracheni abbiano deciso di unirsi all'Is: una tesi è che i primi lo giudichino un "utile idiota", attraverso cui comandare; la tesi contra-

L'Is ha una propria economia di Stato, si basa sullo sfruttamento intensivo dei propri territori occupati e su una diversificazione produttiva (per citarne una, l'anfetamina contro la paura – il Captagon – significa denaro contante da vendere agli angoli dei marciapiedi di tutto il mondo). Per le entrate di Bilancio, ricorre anche a tributi molto peculiari e "creativi", frutto dell'illegalità e dell'estorsione. Ma per certi versi – ben lontani dalla volontà di sembrare blasfemi – ogni mondo è paese: con il SEC 2010, anche nella contabilizzazione del nostro Pil rientrano voci appartenenti all'illegalità. E se lo fanno paesi occidentali avanzati, secondo le linee-guida di Eurostat, perché non dovrebbe farlo lo Stato Islamico?

Così, mentre quest'ultimo ha propri apparati, delle istituzioni, una propria economia, un articolato sistema di tassazione/estorsione e di gestione dei bottini di guerra, al-Qaeda pratica ancora oggi lo sfruttamento della concessione del marchio a diversi gruppi che, a loro volta, devono essere dotati di autonomia finanziaria.

Secondo un approccio moderno, l'Is fa molto affidamento sulle strategie di comunicazione, nelle sue forme più attuali e a seconda dei segmenti di pubblico cui intende rivolgersi: dall'Occidente alla *jihād*[25].

Fra gli ulteriori elementi di differenziazione rispetto ad al-Qaeda vi sono inedite fonti di finanziamento (cfr. par. 3).

A differenza di quest'ultima, oggi l'Is trova forte *appeal* nel mondo musulmano con il suo messaggio tranquillizzante e foriero di elevate aspettative. Finalmente il ritorno al Califfato (venuto meno nel 1924) e

---

ria è che ex appartenenti del regime di Hussein si siano uniti all'Is per trovare mezzi di sostentamento.

[25] Nel 2014 lo Stato Islamico ha fondato l'*Al Hayat Media Center*, rivolto ai popoli occidentali e pubblica materiale in inglese, tedesco, russo e francese. Nel 2014 ha anche fondato la *Anjad Media Foundation*, che pubblica *Anasheed*, ovvero "canti religiosi" che incitano al *jihād*. Lo Stato Islamico si avvantaggia regolarmente dei media sociali, in particolare di Twitter. Per distribuire il suo messaggio, organizza campagne *hashtag*, incoraggiando tweet con etichette popolari e utilizzando applicazioni che abilitano lo Stato Islamico a diffondere la propria propaganda sui profili dei suoi sostenitori. L'uso dei media sociali è stato descritto da un esperto come «probabilmente più sofisticato di [quelli della] maggior parte delle compagnie statunitensi». Ulteriore osservazione al riguardo è che «l'ISIS mette più enfasi nei media sociali rispetto agli altri gruppi *jihadisti* […] Ha una presenza sui media sociali molto coordinata».

all'età dell'oro dell'Islam: il nuovo Califfato appare nell'immaginario di tanti sunniti come una promettente entità (geo)politica che sorge dalle braci di guerre e di distruzione.

Dunque, l'Is sembra più forte e più pericoloso di quanto non lo fosse in occasione della proclamazione del Califfato, nel giugno 2014, con al-Baghdadi divenuto califfo, terrorista munito di PhD in Studi islamici.

Anzi, è divenuto il gruppo terroristico più importante e ricco del mondo.

Anche la megalomania del califfo può essere letta in chiave moderna: la globalizzazione diventerà una globalizzazione islamica. E perché non dovrebbe crederci, se in pochi anni ha realizzato un progetto – la rinascita del Califfato con un esercito di proseliti (manipolati per lo più)[26] – che, secondo bin Laden, avrebbe potuto concretizzarsi solo attraverso un processo secolare?

### *3.1. Il proselitismo*

Una volta reclutato, il *foreign fighter*, se/quando tornerà a casa[27], diventerà un'importante sorgente di reclutamento. Per alcuni, i combattenti stranieri sono degli "eroi moderni". Anche in questo caso, l'immaginario entra in azione.

E persino i raid non sembrano avere effetti deterrenti sul reclutamento, anzi: le fonti dei servizi statunitensi hanno rivelato che, nonostante (o, forse, proprio per) gli attacchi aerei, le reclute dell'Is sono aumentate.

---

[26] Per un approfondimento su questi temi, si vedano K. BHUI, Y. IBRAHIM, *Marketing the "radical": Symbolic communication and persuasive technologies in jihadist websites*, in *Transcultural Psychiatry*, 2013.

[27] Infatti, uomini e donne, che partono verso un nuovo destino avvolto da un'aurea ieratica e che legittimano loro la conquista del paradiso, si ritrovano in realtà nell'inferno. Le donne ridotte in schiavitù sessuale; gli uomini in fuga, fucilati. Tragedia della sorte, la *jihād* digitale sembra seduttiva soprattutto nei confronti delle donne, da Denver a Parigi. I reclutatori sono, infatti, particolarmente abili a gestire la conversazione attraverso i *social network* così da indurre le ragazze adolescenti a cercare felicità, un marito e dei figli nel Califfato. M. MOLINARI, *Il Califfato del terrore. Perché lo Stato islamico minaccia l'Occidente*, Milano, 2015.

L'espressione di forza del raid si accompagna alla potenza del web, il "raid virtuale".

Il cyberspazio è allo stesso tempo un ulteriore *asset* di cui si sono impadroniti gli integralisti islamici di seconda generazione e un nuovo ulteriore teatro di guerra: *1)* la strumentazione tecnologica di cui si servivano Bin Laden e al Zarqawi appare rozza e arcaica al confronto dei *social network* d'ultimo grido e il *dark/deep web* usati dall'Is; *2)* le parti avversarie schierano le proprie "potenze di fuoco", dove entrano in campo organizzazioni quali Anonymous o la Cyber-armata del Califfato.

In realtà, comprendendo l'importanza della *jihād* elettronica, già bin Laden (da cui l'Is ha plagiato l'idea), chiedeva alle cellule di reclutare chi dimostrasse interesse per gli hacker, ai fini di distruggere i siti Internet del nemico e infiltrare le sue rocche strategiche, nella convinzione che "la guerra elettronica è uno strumento efficace della guerra del futuro". Sarebbe al-Britan – nome di battaglia, nato a Birmingham e volontario in Siria, e che aveva già hackerato l'account gmail di Tony Blair – ad aver creato il team di *jihādisti* cibernetici riuscito a scrivere il programma di software criptato che consente oggi al "*cyber*-Califfato" di esistere sui *social network* di tutto il mondo[28].

La conversione tramite web è qualcosa di davvero incontrollabile.

Anche i fondi arrivano dal web.

In realtà, il web sta diventando uno dei nostri peggiori nemici, nel molteplice uso in cui la *jihād* lo utilizza contro l'avversario, occidentale e non.

In risposta, l'Europa sta combattendo tale *appeal* con una contro-narrativa domestica anti-*jihādista*: in Belgio, essa sostiene la creazione di un gruppo di esperti di comunicazione che aiuterà gli Stati membri a contrastare la propaganda fondamentalista, che fa proseliti sul web, con una contro-informazione mirata[29]. Infatti, solo una piccola parte dei

[28] M. MOLINARI, *op. cit.*

[29] La UE, attraverso finanziamenti comunitari, sta creando in Belgio un gruppo di esperti di comunicazione (*Syria strategic communications advisory team - Sscat)*, che aiuterà gli Stati membri a scambiare buone pratiche e a capire come contrastare la propaganda fondamentalista (che fa proseliti sui forum dei *social media*) attraverso una contro-informazione mirata.

combattenti si addestra all'estero: il problema è soprattutto il "terrorismo domestico" fomentato da Internet (piuttosto che nelle moschee come ai tempi di al-Qaeda).

## *4. L'innovatività delle fonti di finanziamento del Califfato*

Ci limiteremo ad analizzare le principali fonti di finanziamento[30], specificatamente quelle inedite rispetto a quanto si avvaleva la *jihād* della generazione precedente. Alcune sono lecite, altre no, altre ancora vengono "sporcate" dall'uso distorto.

Come ogni Stato, quello Islamico ha bisogno di finanziarsi tramite tributi. Esempi sono la *jizya* e la *khums*. La prima è prevista dalla *sharia* come un'"imposta di protezione", anche c.d. "religiosa". I cristiani che vivono in aree sotto il controllo dell'Is, hanno quattro opzioni: convertirsi, andare via, pagare la *jizya*, l'esecuzione. Chi accetta di pagare, diventa *dhimmi*, cioè un protetto assoggettato al potere musulmano locale. L'importo è equivalente a 720 dollari all'anno[31]. La *khums* è un tributo previsto dalla legge islamica, per la quale si è obbligati a versare allo Stato una quota del valore dei beni provenienti dalla terra. E qui la fantasia abbonda: il tributo deve essere pagato da parte di chi depreda il patrimonio archeologico ai fini di contrabbando. L'importo del "tributo-estorsione" varia tra regioni e a seconda dell'oggetto recuperato. La *zakat*, tipicamente un'entrata legale – sfruttata anche da al-Qaeda – che, secondo la legge islamica, ha un'aliquota pari al 2,5% della ricchezza dell'individuo, nello Stato Islamico sale al 10%, per finanziare la guerra.

E, sempre in tema di estorsioni, c'è il *business* delle multe, salatissime, ad esempio, se di notte si attraversa il deserto con le luci posteriori che non funzionano.

E poi i pedaggi dell'autotrasporto commerciale che attraversa i territori controllati, tassati tra il 10 e il 15%, dietro ricatto di far esplodere il

[30] Per un'analisi, si rinvia a M. FIOCCA, S. COSCI, *La dimensione finanziaria del terrorismo e del contro-terrorismo transnazionale*, Catanzaro, 2004.

[31] M. MOLINARI, *op. cit.*

carico. Inoltre, secondo il copione mafioso, mazzette per la protezione delle attività produttive e commerciali[32].

E poi c'è il petrolio, che per l'Is rappresenta un'eccezione rispetto alle altre realtà terroristiche. Il petrolio di contrabbando proviene dai pozzi controllati dall'Is: il 60% di quelli siriani e circa 350 in Iraq. I trafficanti lo fanno arrivare in Turchia, Giordania e Kurdistan, dove vi sono gli acquirenti che, nel mercato parallelo, lo pagano 40 dollari al barile, oltre 30 dollari in meno rispetto al prezzo ufficiale di mercato[33]. Da decine di interviste con commercianti siriani, tecnici, *intelligence* occidentale ed esperti di petrolio, l'Is ha costituito un'organizzazione simile ad un'impresa petrolifera di Stato – che si avvale dei migliori ingegneri e manager che riesce a reclutare in tutto il mondo –, che continua a crescere e a specializzarsi.

Inoltre, come predice la teoria economica per il mercato in regime di monopolio, l'impresa pratica una politica dei prezzi differenziata, a seconda dei mercati e degli utenti, in modo da massimizzare i profitti.

Sull'economia del petrolio si basa lo Stato Islamico. La centralità del suo ruolo è confermato dal fatto che in uno Stato molto decentrato, qual è l'Is – dove gli amministratori dei governi sub-centrali amministrano secondo la *shura* centrale – rimangono a livello centrale alcune funzioni cruciali: il petrolio, la propaganda, le operazioni militari.

Malgrado i giacimenti siano presidiati, esiste un rilevante mercato parallelo, e quindi la rete di connivenze è molto capillare e robusta.

Finora, la minaccia più significativa è stata il prosciugamento dei più vecchi giacimenti siriani, non disponendo l'Is delle capacità tecnologiche occidentali per contrastare questo calo. Inoltre, esso può venderne di meno, dovendolo allocare per le operazioni militari.

In Medio Oriente, un circolo vizioso che si perpetua tra parti avversarie: il controllo del petrolio per finanziare la guerra; la guerra per il controllo del petrolio e, quindi, il tentativo – fra gli obiettivi da colpire – di lasciarli intatti per poterli gestire in futuro.

Altra fondamentale risorsa economica – probabilmente la seconda – è il trafugamento del patrimonio culturale di importanza mondiale. Lo

[32] M. VALSANIA, *L'economia sommersa di ISIS: da estorsioni al commercio di petrolio affari per milioni di dollari al mese*, in *Il Sole 24Ore*, 28.08.2014.

[33] M. MOLINARI, *op. cit.*

Stato Islamico è in guerra non solo contro la Siria o l'Iraq; il suo nemico è l'identità culturale di questi paesi, le loro radici, le loro tradizioni, i loro posti. Nella città di Hatra, che risale al III secolo A.C., l'Is ha usato il meraviglioso palazzo reale per immagazzinare armi e munizioni, per addestrare combattenti e giustiziare i prigionieri. Nell'immaginario collettivo, essa rimarrà tutto questo. E ancora la stupenda Chiesa Verde, di Tikrit, una struttura suggestiva scavata nella roccia, saccheggiata e poi distrutta dai terroristi.

Molto richiesto sul mercato nero dell'arte, essi non si limitano a distruggere il patrimonio storico, ma lo usano per finanziare la guerra. Una conferma indiretta della crescita del mercato nero di reperti antichi arriva dagli Stati Uniti. Le importazioni americane di antichità provenienti dal Medio Oriente sono aumentate vertiginosamente tra il 2011 e il 2013. Secondo i dati forniti dalla *US International Trade Commission*, in soli tre anni le importazioni da Egitto, Iraq, Libano, Siria e Turchia sono cresciute dell'86%, passando da un valore di 51,1 milioni di dollari a 95,1 milioni di dollari[34].

Questa non è la prima volta che lo sconfinato patrimonio culturale della regione è minacciato. Il saccheggio peggiore fu durante la conquista mongola di Baghdad, nel 1258. La tradizione racconta che allora il fiume Tigri si tinse di rosso per il sangue di migliaia di morti e di nero per l'inchiostro di migliaia di manoscritti; eppure la barbarie dei mongoli impallidisce a confronto di quella dello Stato Islamico.

Inoltre, il Califfato conta su un enorme patrimonio immobiliare assai prestigioso con la presa di Mosul e, quindi, sulle relative locazioni.

La ricchezza dell'Is, a differenza degli altri gruppi terroristici, viene così dall'interno. Per questo motivo è difficile utilizzare gli strumenti

[34] Da strumenti inediti usati dai terroristi alle risposte inedite e d'avanguardia, come quella che potremmo definire di *cyberarcheologia*. Cioè, ricostruire copie virtuali di capolavori dell'arte perduti, per salvarne la memoria nel cyberspazio. È l'obiettivo del *Project Mosul*, una raccolta in *crowdsourcing* delle foto dei tesori archeologici del Museo di Mosul (Iraq), scattate prima che queste venissero distrutte nel corso dell'attuale conflitto. L'idea è raccogliere il maggior numero possibile di scatti dei reperti scomparsi per ricavarne, grazie a una speciale tecnica fotografica, fedeli modelli in 3D, virtuali e indistruttibili.

tradizionali già sfruttati contro al-Qaeda, come il blocco dei depositi bancari sospetti.

La scaltrezza e le abilità manageriali fanno sì che i suoi traffici coinvolgano intermediari e compratori di paesi o regioni formalmente nemici: dai curdi agli sciiti iracheni, dagli iraniani fino ai turchi[35].

In una moderna prospettiva di "operazione trasparenza", fin dal 2012 l'Is ha prodotto rapporti annuali fornendo una *vision* e i dati sulle proprie operazioni con una metodologia che richiama report aziendali, allo scopo soprattutto di incoraggiare i potenziali donatori[36].

Lo Stato Islamico ha bisogno di risorse non tanto per gli attacchi terroristici: essi richiedono più un'attività di pianificazione che risorse economiche per la loro realizzazione. Infatti, il dato comune degli attacchi terroristici effettuati nel 2015 dall'Is in Europa è che essi sono stati perpetrati da affiliati appartenenti alla piccola criminalità, con precedenti legali e che con la loro attività si autofinanziano. Quindi, l'Is, come già al-Qaeda, si avvale del connubio criminalità-terrorismo. Dov'è lo spazio per la religione musulmana in tutto ciò? E, infatti, non c'è: atei, agnostici, ebrei, cristiani ingrossano le fila del Califfato.

Tale *network* ha due importanti corollari: i costi che sono costretti a sostenere i paesi aggrediti nel tracciare e colpire tanti piccoli rivoli; la triplice conoscenza da parte dell'*intelligence* della criminalità, del terrorismo e della corruzione.

Le risorse sono necessarie alla sopravvivenza dello Stato stesso. Vale a dire, per il controllo del territorio, per riparare le infrastrutture distrutte dai raid, per la difesa e la manutenzione degli impianti petroliferi, per l'acquisto di armi, per i campi di addestramento, per le retribuzioni dei miliziani, per la propaganda, per il mantenimento dell'ampio apparato amministrativo, del sistema di *welfare* insieme alle scuole e ad altri servizi sociali, per la realizzazione di armi di distruzione di massa di vario genere e della tecnologia informatica, per le remunerazioni degli esperti che figurano sul libro paga.

---

[35] M. VALSANIA, *op. cit.*

[36] R. KHALAF, S. JONES, *Selling terror: how Isis details its brutality*, in *Financial Times*, 17.06.2014.

## *5. L'economia della paura: una paura "liquida"*

Forse la metafora che più si attaglia alla paura di questo terrorismo è la "sindrome del Titanic"[37], cioè che un imponente congegno – apparentemente dotato di una indiscutibile resilienza – improvvisamente si riveli sotto gli occhi di tutti "sottile come un'ostia" e si frantumi, lasciando precipitare una collettività nella profonda e gelida oscurità del nulla, dove non esiste più niente di ciò che rappresentava le proprie sicurezze e ancore, le "basi elementari" di una vita organizzata sulla base di *routine*, regole, stili di vita. Ma il vero orrore non è l'*iceberg*; il vero orrore è quello che accade dentro il transatlantico, in apparenza rutilante e arrogante ma nei fatti privo di sicurezze basilari, quali un numero adeguato di scialuppe. Insomma, l'orrore di non essere sufficientemente attrezzati di fronte a qualcosa che ci viene improvvisamente contro per sopraffarci.

Quanto, noi aggrediti, siamo equipaggiati per affrontare il nostro *iceberg*? Siamo in guerra, e lo sappiamo; ma abbiamo sufficiente resilienza?

Il fattore più rilevante è l'attuale crisi di fiducia, cioè la presa di consapevolezza che il male si può nascondere ovunque, perché non ha una carta d'identità – se non falsificata e, quindi, non riconoscibile – e quindi può mimetizzarsi nella folla. Che chiunque può essere reclutato per la propria causa, in servizio effettivo, in congedo temporaneo (dormiente) o potenzialmente arruolabile[38]. Anzi, con gli attentati del 2006, i britannici hanno dovuto prendere atto che il nemico era tra loro: il nemico erano loro stessi[39].

Qual è il costo di questa paura? E come esso si impenna quando viene confermato da più fonti che l'Is dispone di armi di distruzioni di massa?

Esplorare le conseguenze economiche del terrorismo è una sfida nella misura in cui la paura destruttura il quotidiano, la normalità e la *routine* e riguarda il costo(-opportunità) che gli individui annettono al cambiamento. Quindi, c'è una forte componente soggettiva nella quan-

[37] Z. BAUMAN, *op. cit.*

[38] Z. BAUMAN, *op. cit.*

[39] D. MOÏSI, *L'Europa della paura*, in *Aspenia*, n. 71, 2015.

tificazione di tali costi. Potremmo parlare dell'elasticità della domanda di "normalità" rispetto al costo della paura (punto 3.1).

Proprio perché la paura è un fattore estremamente complesso e soggettivo, è difficile prevedere il possibile impatto sulla domanda aggregata, sulla domanda di politiche pubbliche, sui mercati finanziari e valutari, e così via.

Ma ormai, alcune lezioni le abbiamo apprese, cosi come i canali attraverso cui la "paura *jihāddismo*" si trasmette sull'economia[40].

Riguardo alla risposta all'evento ansiogeno, lo spettro è molto ampio a causa di un'informazione asimmetrica tra schieramenti, disponendo il terrorismo di un set informativo più ampio di quello occidentale. L'asimmetria è legata *1)* alla capacità mimetica dei terroristi e delle loro strutture di appoggio; *2)* essi sanno quando e cosa colpiranno; *3)* conoscono l'agenda dei paesi occidentali. Non è viceversa, malgrado l'attività dei servizi di *intelligence*.

Per avere una percezione dell'intrusività – oltre che dei costi – della dimensione di questa guerra, possiamo rifarci ad uno scritto programmatico, un manifesto, riportato da Atran sul *The Guardian*, "La gestione del caos", scritto nel 2004 da un gruppo di al-Qaeda:

> Diversificate ed espandete gli attacchi tesi a tormentare il nemico crociato-sionista in ogni luogo del mondo islamico, e anche al di fuori di esso se possibile, così da disperdere gli sforzi del nemico e dissanguarlo il più possibile.
> Se una località turistica frequentata dai crociati viene colpita, tutte le località turistiche del mondo dovranno adottare misure di sicurezza aggiuntive che comporteranno un enorme aumento delle spese.

Dunque un'emergenza complessa, la cui risposta richiede: *a)* prevenzione dei rischi per la sicurezza; *b)* adeguata preparazione al possibile attacco; *c)* adeguata preparazione alle reazioni agli attacchi, per gestirne ed attenuarne le conseguenze, tra cui le strategie di comunicazione in situazioni di emergenza; *d)* perseguimento dei reati e dei loro autori; *e)* controffensiva, non solo di *hard power*, ma anche di *soft*

[40] M. FIOCCA, *L'economia della paura*, in AA.VV., *Terrorismo: impatti economici e politiche di prevenzione*, Milano, 2006; M. FIOCCA, *L'economia della paura*, in *Limes*, n. 10, 2016.

*power* (missioni di pace, controllo del territorio nemico e ricostruzione dei *failed States*, dove sono localizzate miniere di nemici occidentali, tra cui i *foreign fighter*); *f)* diffusione della contro-narrativa; *g)* ricostruzione; *h)* coordinamento fra le forze alleate nei vari settori (*intelligence*, ecc.).

Sono innumerevoli le misure – anche a livello di coordinamento internazionale (quale un'*intelligence* europea, attraverso la costituzione di un'Agenzia *ad hoc*, che rafforzerebbe le strutture dell'Unione, sempre che si riescano a superare gelosie e nazionalismi) – che si dipanano da questa tassonomia, qui molto semplificata.

Ci limiteremo a considerare solo alcuni aspetti: l'impatto sulla finanza pubblica, sulla macroeconomia e sulla micro; sul settore reale e su quello finanziario.

Nel campo dell'economia pubblica, la collettività richiede maggiori politiche per la sicurezza (per loro stessi, per le infrastrutture, per i sistemi informatici, contro un eventuale "tsunami digitale", e per tutto ciò che garantisce il proprio quotidiano).

In un contesto di risorse scarse e di revisione della spesa pubblica, questo comporta una nuova prioritizzazione delle politiche pubbliche, a pregiudizio di altre.

L'intervento pubblico per la sicurezza significa naturalmente anche una politica per i profughi di guerra. Tuttavia, essi pesano sui nostri consumi collettivi e sui nostri sistemi di *welfare*. Da qui il dibattito di inserire nella *governance* europea anche una Clausola sugli immigrati.

Per le politiche economiche – fiscali e monetarie –, possiamo riportarci alle lezioni apprese all'indomani dell'11/9, dove sono state varate politiche fortemente espansive. Per quella monetaria, questo sta accadendo anche oggi, su entrambe le sponde dell'Atlantico; per le politiche fiscali, nell'eurozona, dopo un'epoca di rigida impostazione (prociclica) basata sulle regole numeriche, si è riconosciuta l'esigenza di una minore austerità, che nel 2015 la Commissione ha battezzato come un "consolidamento fiscale amico della crescita".

A livello macro, gli investitori attribuiranno un minor merito di credito al paese colpito (rischio-paese), con un innalzamento dei tassi di interesse e un ampliamento dello *spread*. È quindi ipotizzabile una fuga di capitali (*flight to quality*), con un conseguente indebolimento della

valuta, a pregiudizio della bilancia dei pagamenti e della disponibilità di capitali per il finanziamento degli investimenti del paese aggredito. La riduzione dello stock di capitale (elemento fondante per la crescita del paese e per l'innovazione) viene da più parti: oltre che dalla sua probabile distruzione fisica connessa all'attacco, dalla riduzione degli investimenti diretti esteri (IDE).

Ma anche quando i tassi di interesse fossero vicino allo zero – com'è attualmente –, gli *animal spirits* non investirebbero a causa del clima di sfiducia e di una bassa redditività attesa. Quindi, nell'ambito dell'economia reale, si può prefigurare una riduzione della domanda interna (consumi delle famiglie e investimenti delle imprese), con ricadute negative sulla componente ciclica e sull'*output gap*, e con il persistente rischio di deflazione.

Maggiore volatilità dei mercati finanziari e valutari, destabilizzazione dovuta all'*herd behaviour*, bolle o scoppio delle stesse, attacchi speculativi, fenomeni di panico, corsa agli sportelli, possibili effetti domino e di *spillovers*. Questi ed altri ancora sono gli effetti stilizzati connessi ad un'emergenza. Eppure, tramite le lezioni apprese con la prima ondata di *jihāddismo*, i mercati sono rimasti relativamente stabili e l'intero settore finanziario si è avvalso di una maggiore resilienza.

Sul piano micro, in tempi di incertezza pervasiva, viene rivista l'allocazione del reddito fra risparmio e consumo. Ma al di là dell'incertezza, a favore del risparmio può giocare un ripiegamento su stessi ascrivibile a ferite profonde e permanenti – proprio ciò che vuole lo *jihāddismo.* Esse rimettono in discussione tutto ciò che per noi finora non era questionabile e che stimolano la percezione di mutamenti intorno a noi così radicali e dell'esistenza di altri "mondi", che prima sembravano tanto lontani da non vedere neppure.

E proprio sul solco di questo spirito, cambia anche il paniere di consumi, a pregiudizio di quelli di lusso. Ciò anche per un'altra ragione, meno intimista ed esistenziale, ma di natura economica: con la riduzione del turismo, si riduce il *travel retail*, costituito prevalentemente da tale categoria di beni. Anche il *leisure time* viene speso in modo diverso, a favore dell'*home entertainment*.

Nell'attuale fase, sembra che invece venga a mancare la domanda di beni-rifugio.

### *5.1. Le abitudini di consumo*

La paura e l'insicurezza, nella misura in cui impongono un aggiustamento delle abitudini, hanno un costo(-opportunità): quello del cambiamento. Nel caso di *routine*, prassi, stili di vita, abitudini più radicate, con scarsa avversione al rischio, il costo dell'aggiustamento è naturalmente più elevato. I soggetti con *pattern* di consumo e abitudini ben definiti e specifiche preferenze al rischio, saranno meno disponibili al cambiamento a causa del costo ad esso associato. Si può pensare quindi alle abitudini di consumo come ad una particolare categoria di beni necessari (in contrapposizione a quelli di lusso): anche quando aumenta il loro costo, il consumatore tende a non alterarne la domanda. Se accettiamo tale ipotesi, ne discende che l'elasticità dei beni che costituiscono le abitudini, le tradizioni, gli stili di vita, la *routine* di un determinato individuo è bassa rispetto al "prezzo della paura".

Se questo è vero, le preferenze del soggetto si identificherebbero perfettamente nel messaggio lanciato ai mercati (e non solo i mercati, ma anche gli individui vivono di *signalling*) all'indomani dell'attentato a Londra del luglio 2005: "Keep going, business as usual".

Poiché, ovviamente soggetti diversi presentano sentieri di consumo/abitudini diversi, questa particolare categoria di beni necessari è del tutto soggettiva, come lo è la risposta alla paura. C'è chi dopo un attentato in metropolitana o in stazione ferroviaria torna a servirsi degli stessi mezzi di trasporto, cioè torna alla *sua* "normalità", c'è invece chi li eviterà per anni.

In sintesi, poiché è soggettiva tale categoria di beni necessari, sarà diversa e soggettiva anche la loro elasticità al "prezzo della paura".

Per esprimere lo stesso concetto, sempre in termini economici, tipicamente si parla di *trade-off* tra libertà e sicurezza, e tuttora molte persone non sembrano disposte a cedere pezzi di libertà in cambio di una maggiore sicurezza.

## *6. Le contro-misure di mitigazione del rischio di natura finanziaria: l'attività del FATF-GAFI*

Il quadro normativo internazionale di prevenzione e contrasto al finanziamento del terrorismo è caratterizzato dalle misure dettate dalla Convenzione internazionale contro il finanziamento del terrorismo dell'8 dicembre 1999, dalle Risoluzioni adottate dal Consiglio di sicurezza delle Nazioni Unite ai sensi del Capitolo VII della Carta, dalla normativa comunitaria e dalle Raccomandazioni del GAFI-FATF.

Le misure restrittive si sostanziano nel congelamento dei fondi e delle risorse economiche detenute da persone fisiche e giuridiche, gruppi ed entità specificamente individuati dalle Nazioni Unite e dall'Unione europea (soggetti "designati").

Costituito nel 1989 dal G-7, com'è noto, il GAFI-FATF è un organismo intergovernativo con lo scopo di ideare e promuovere strategie di contrasto al riciclaggio dei capitali di origine illecita. Nel 1990, emanava le 40 Raccomandazioni che costituivano un insieme minimale di misure anti-riciclaggio necessarie per contrastare il fenomeno e rafforzare la cooperazione internazionale.

Dal 2001 – a pochi giorni di distanza dagli attentati di New York – gli è stato affidato anche il mandato di prevenzione del finanziamento al terrorismo. Di conseguenza, ha emanato 8 Raccomandazioni Speciali (9 dal 2004) dedicate specificamente al finanziamento del terrorismo. Tali Raccomandazioni, oltre a fornire linee di indirizzo per rendere operative le Risoluzioni ONU, hanno definito alcuni standard regolamentari per meglio presidiare sul piano normativo alcuni settori ritenuti maggiormente esposti al rischio di finanziamento del terrorismo (servizi di *money transfer*, bonifici transfrontalieri, trasferimenti di contante al seguito, operatività di organizzazioni non-profit).

Sulla base del connubio tra attività finanziarie illecite e finanziamento del terrorismo, il GAFI *1)* analizza le tecniche e l'evoluzione delle attività finanziarie illecite; *2)* valuta e monitora i sistemi nazionali, individuando i paesi con lacune nei loro sistemi di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo. A tale scopo, utilizza anche lo strumento informativo e dissuasivo delle liste delle giurisdizioni non cooperative, le c.d. liste *Name and shame*, in modo da

fornire al settore finanziario elementi utili per le analisi del rischio e da indurre i paesi "additati" a conformarsi almeno ai requisiti minimi richiesti dalla regolamentazione – apertura e trasparenza – al fine di evitare l'emarginazione da parte della comunità internazionale.

Il metodo delle liste è praticato anche dall'OCSE (nell'ambito dell'*Harmful tax competition*). Vi sono forti legami e sinergie fra le due liste – che vengono periodicamente aggiornate – per il forte nesso fra le distorsioni di natura tributaria e quelle nel settore finanziario. Infatti, i paradisi fiscali, di cui si occupa la lista dell'OCSE, sono centri dove vengono a combinarsi le disfunzioni nel settore fiscale e in quello finanziario. Circostanza che li rende particolarmente vulnerabili/appetibili al terrorismo, oltre che alla criminalità.

Il principio alla base di entrambe le liste sta il fatto che in un contesto globale di forti interdipendenze, la circostanza che una giurisdizione non cooperi mina significativamente l'efficacia delle misure di contrasto.

Nel 2008, il mandato del GAFI è stato esteso anche al contrasto del finanziamento della proliferazione di armi di distruzione di massa. L'attuale mandato scadrà nel 2020.

Nel febbraio 2012, le Raccomandazioni Speciali sono state trasfuse nelle nuove 40 Raccomandazioni, che comprendono nel loro campo d'azione la prevenzione e il contrasto del riciclaggio, del finanziamento del terrorismo e del finanziamento dei programmi di proliferazione delle armi di distruzione di massa.

Del GAFI fanno parte 36 membri in rappresentanza di Stati e organizzazioni regionali, nonché, come osservatori, rilevanti organismi finanziari internazionali e del settore (tra i quali Nazioni Unite, Fondo Monetario Internazionale, Banca Mondiale, Banca Centrale Europea, Europol, Egmont).

## *7. Conclusioni*

Alcune notazioni per concludere.

La prima.

La geostrategia ha troppe stratificazioni per capire quelle più profonde.

In Siria si sta perpetrando una guerra nella guerra in cui non si capisce chi combatte contro chi.

Uno spunto è dato dalla polemica tra USA e Russia contro i raid di quest'ultima sulla Siria di inizio ottobre 2015, che – nelle accuse del Presidente statunitense – hanno colpito anche i ribelli dell'Esercito libero siriano, armati e addestrati dalla CIA.

La Russia: chi effettivamente appoggia, al di là delle dichiarazioni di intenti nel corso dell'assemblea generale delle Nazioni Unite del 28 settembre 2015? Chi vuole colpire effettivamente al di là della sua proposta di una coalizione internazionale contro lo Stato islamico, "come quella contro Hitler", a cui dovrebbero partecipare gli occidentali, i paesi arabi, i russi e il governo siriano?

E nell'altra sponda dell'Atlantico, qual è il problema di Obama verso Assad, nei confronti del quale l'atteggiamento è ondivago? È forse in parallelo con la disponibilità di petrolio nei giacimenti statunitensi? Quando essa è abbondante, è interesse USA destabilizzare la Siria, quindi il Medio Oriente, provocando l'aumento del corso del greggio, da cui si approvvigiona la Cina, un *competitor* forte degli Stati Uniti.

Inoltre, secondo le accuse della Russia, la Turchia compra petrolio di contrabbando dall'Is e sulla c.d. Autostrada della *jihād* (il lembo di terra a sud della Turchia) vi passano le reclute agganciate tramite web, da addestrare in Siria e in Iraq.

Eppure, la Turchia già appartiene alla NATO e sta preparando le carte per entrare nella UE, dopo il primo infruttuoso tentativo del 2005.

Ancora, quanti di questi paesi che siedono al Tavolo dei nostri alleati, come il Qatar – con la sua storica *Al Udeid Air Base* –, stanno cercando di "esternalizzare" il terrorismo, finanziandolo, purché non col-

pisca i propri bersagli sensibili? Si sospetta che il principale finanziatore dell'Is, tra il 2013 e il 2014, sia stato il Qatar[41].

Non a caso i sospetti nutriti dalla Francia nei confronti dell'Arabia Saudita e delle altre petromonarchie del Golfo, che sembrano simpatizzare per lo Stato Islamico e foraggiarlo. Se ciò fosse vero, non saremmo poi molto lontani dal modello di al-Qaeda, sponsorizzato dagli Stati canaglia; l'impianto autarchico dello Stato Islamico sembrerebbe di conseguenza un *bluff*; lo stesso Stato islamico sembrerebbe un *bluff*. E di *bluff* in *bluff*, lo stesso *jihādista* ispira nient'altro che questo. Tuttavia, si tratta di un *bluff* che uccide.

Ma viene il sospetto: l'esistenza dello Stato Islamico, la sua potenza, le sue dimensioni, la sua ricchezza (di oltre 2 miliardi di dollari)[42], non sono funzionali ad interessi, conflitti e coalizioni che si giocano, a livello internazionale, su altri tavoli?

Tanti intrecci, tanti interessi, tanta disinformazione al di sotto delle proclamatorie, tanta incertezza, tanti giochi e sottogiochi.

Altro è difficile da aggiungere.

La seconda notazione.

Il fenomeno del cyberterrorismo è destinato ad essere sempre più pericoloso: esso infatti è economico, anonimo, può essere condotto a distanza, ha a disposizione una quantità impressionante di obiettivi, rende facile il reclutamento e il *fund raising*, può colpire, anche se non sempre in modo letale, un numero estremamente ampio di obiettivi e, infine, è capace di generare una copertura molto maggiore da parte dei mezzi di comunicazione, obiettivo – questo – particolarmente ricercato da parte dei terroristi.

Recentemente si è venuto a scoprire che i lupi solitari non sempre sono tanto solitari, in quanto esistono i c.d. *virtual planner*, che individuano i potenziali attentatori e li aiutano a organizzare e coordinare gli attacchi, scegliendo gli obiettivi, determinando la tempistica, fornendo assistenza tecnica. Tale modello rivoluzionario di radicalizzazione dell'Is, fallito con al-Qaeda per insufficienza tecnologica, prende il nome di *remote intimacy*.

[41] M. MOLINARI, *op. cit.*

[42] M. CHULOV, *How an arrest in Iraq revealed Isis's $2bn jihadist network*, in *The Guardian*, 15.06.2014.

Il terrorismo islamico attuale è in grado di impadronirsi – fra gli *asset* occidentali – delle più moderne tecnologie informatiche. Ciò si traduce in un continuo rincorrersi tra nemici, con l'Occidente che tende a produrre – ad uso preventivo e repressivo – tecnologie sempre più sofisticate e normative, queste ultime bellissime architetture del legislatore, che accompagnano e si sviluppano in parallelo a tale fenomeno.

Ma arriva ineludibilmente il momento in cui i contenuti normativi devono essere implementati e quindi tradursi in politiche pubbliche per la sicurezza, richieste dalla collettività, nell'ambito delle misure di prevenzione, gestione dell'emergenza e repressione.

Terza notazione.

La realizzazione della politica pubblica deve passare il doppio test dell'efficienza (ottimizzazione vincolata) e dell'efficacia, che riguarda la sua adeguatezza rispetto agli obiettivi che si propone.

A tale scopo devono essere costruiti indicatori di *performance* o di risultato anche di natura quantitativa, basati quindi su metodologie economico-statistiche.

Nell'attuale contesto generalizzato di revisione della spesa (*spending review*), tale programma richiederà un ri-orientamento dei programmi di spesa, vale a dire una revisione delle priorità e, quindi, una diversa allocazione della spesa pubblica.

Secondo le più recenti misure della *governance* economica europea, per la realizzazione di tali programmi, lo Stato membro può appellarsi alle recenti Clausole che legittimano un temporaneo scostamento dal percorso di avvicinamento verso 'Obiettivo di Medio Termine' (OMT) e, quindi, una giustificazione di un rallentamento nel consolidamento dei conti pubblici. Vale a dire che lo Stato membro può chiedere alla Commissione europea di avvalersi della Clausola degli investimenti o alla Clausola per le riforme strutturali, richiesta che sulla base di una serie di parametri la Commissione può accettare o rigettare.

Quarta notazione.

*Follow the money* era l'indicazione di Giovanni Falcone per colpire la mafia; tecnica di indagine mutuata per il terrorismo. Tracciare la mappatura dei flussi finanziari è un'operazione complessa, sofisticata, ad elevata tecnologia ovvero, in alcune circostanze, *naïve*; tuttavia, dirimente.

Il *money transfer* riesce a raggiungere un piccolo villaggio sperduto dall'altra parte del mondo – assolvendo l'importante funzione di "inclusione finanziaria" – a costi contenuti, laddove il sistema bancario non riuscirebbe. In tal senso, è in grado di superare un *market failure*, e va quindi preservato.

Ma, quando i suoi punti di forza diventano anche quelli della criminalità e del terrorismo, i sistemi di *money transfer* vanno regolamentati e monitorati.

Con la *jihād* 1.0, tali trasferimenti – tipicamente le rimesse degli emigrati – si canalizzavano attraverso le c.d. banche dei poveri, quali le *hawala* e le *hundi*. Esse costituiscono un tipico esempio di inclusione finanziaria, di cui anche oggi si serve un gran numero di lavoratori immigrati.

Nella *jihād* 2.0, gli strumenti si sono evoluti: sistemi pseudo-bancari per la movimentazione del denaro tramite i cc.dd. *Informal Value Transfer Systems* (IVTS). Le caratteristiche stesse li rendono particolarmente adatti a trasferimenti, anche di entità elevata, destinati alla criminalità, al terrorismo, alla corruzione.

I rischi di finanziamento al terrorismo non sono collegati solo ai meccanismi di trasferimento del denaro, ma anche ai mezzi di pagamento non regolamentati, quali le valute virtuali. Sebbene tracciate su un registro di transazioni (*block-chain*, *public ledger*), le operazioni in valute virtuali non permettono una sicura identificazione dei soggetti che le eseguono.

Nel 2015, la Banca d'Italia ha posto l'attenzione sull'obbligo di segnalazione degli scambi in valute virtuali a rischio riciclaggio e finanziamento al terrorismo.

Quinta notazione.

Un fenomeno recente con cui l'Europa sta confrontandosi è un massiccio ritorno di *foreign fighters*, Ciò pone ulteriori gravi problemi di sicurezza: si tratta infatti non di autodidatti che hanno scaricato manuali da Internet, ma di soggetti con elevati livelli di addestramento e di *skill*, quindi estremamente pericolosi.

Sesta ed ultima notazione, di natura metodologica.

La forza dell'interdisciplinarietà. Appare oggi scontata per analizzare la complessità del mondo reale, ma già nel 1924 – quando scriveva la biografia di Alfred Marshall – Keynes ne enfatizzava l'importanza[43].

Il presente lavoro è un tentativo in tal senso.

[43] Cfr. *Cambridge economists*, in *The Economist*, 24.12.2016-06.01.2017.

# TERZA SESSIONE

# NUOVE SFIDE TRA TERRORISMO, SVILUPPO TECNOLOGICO E GARANZIE FONDAMENTALI: NOTE INTRODUTTIVE

*Gabriella Di Paolo*

Ringrazio innanzitutto gli organizzatori di questo convegno, il prof. Gabriele Fornasari e il dott. Roberto Wenin, per l'invito, e per aver voluto riservare un'apposita sessione all'analisi degli aspetti strettamente processuali della vasta gamma di misure adottate, a livello nazionale e nel panorama comparatistico, sotto il paradigma della "lotta" al terrorismo. In effetti, se la modernità reca con sé, come effetto delle trasformazioni sociali, anche nuovi fenomeni criminosi, è altresì vero che essa ha messo a disposizione dei sistemi di *law enforcement* anche nuovi, insidiosi, strumenti di controllo sulle attività individuali, che indubbiamente facilitano l'accertamento dei reati e la loro prevenzione.

Per introdurre brevemente l'argomento, mi pare utile riprendere quanto emerso nella sessione di ieri, in particolare nelle parole dell'avv. Beniamino Migliucci, Presidente dell'Unione Camere Penali Italiane (UCPI).

L'avv. Migliucci ha ricordato – e trovo questa considerazione particolarmente pertinente per la nostra prospettiva di analisi, che concerne, come detto, i profili processuali – che interrogarsi sulla disciplina antiterrorismo (ovvero su come i legislatori dei vari Paesi o la Comunità Internazionale hanno cercato rispondere, sul piano penale, al fenomeno del terrorismo) richiede non soltanto di scandagliare le varie fattispecie incriminatrici, per capire se, e fino a che punto, certe condotte possano rientrare nell'area del penalmente rilevante, ma anche di riflettere sull'impatto che la disciplina antiterrorismo ha nella vita di tutti noi, sui nostri diritti e libertà.

E questo perché la storia ci insegna che la maggior parte dei Governi, quando si apprestano a intervenire in questa delicata materia, manifestano una netta propensione a rafforzare i poteri investigativi delle

autorità coinvolte nella "guerra al terrorismo", siano esse autorità di *intelligence* o incaricate di indagini penali[1]. In particolare, il *trend* comune è quello del potenziamento della attività di raccolta e/o apprensione di dati, informazioni, comunicazioni, e, più in generale, il rafforzamento dell'ampio ventaglio di misure investigative speciali riconducibili, secondo la nomenclatura di matrice statunitense, alle categorie della *electronic surveillance* e della *technologically-assysted physical surveillance*. In buona sostanza, si risponde al "terrore globale" instaurando una sorta di controllo globale, di orwelliana memoria[2].

Se questa è la premessa da cui muovere – senz'altro anche con riferimento alla legislazione antiterrorismo più recente – attraverso il contributo dei relatori che mi succederanno si cercherà anzitutto di ricostruire gli strumenti investigativi messi in campo per contrastare il fenomeno del terrorismo internazionale (soprattutto, di matrice islamica). Strumenti investigativi che – è bene evidenziarlo fin da ora – sono pertinenti sia alla stretta prevenzione, che alle indagini penali.

Si cercherà poi di comprendere quali siano le peculiarità (e le criticità) delle indagini in ambiente informatico. Difatti, come s'è notato ieri, le nuove forme di terrorismo tendono a sfruttare le capacità connettive di Internet, della rete: non solo le comunicazioni, ma finanche l'addestramento dei *foreign terrorist fighters* spesso si svolge a distanza, *online.* La lotta a tale fenomeno può quindi necessitare l'oscuramento di certi siti, o l'acquisizione di informazioni relative ai siti web visitati dal

[1] Il pensiero corre, anzitutto, alla legislazione anti-terrorismo statunitense, adottata dopo gli attentati dell'11 settembre 2001. Sul punto sia consentito rinviare a G. DI PAOLO, *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, Milano, 2008, spec. 59 ss., e 67 ss. Cfr. anche J. VERVAELE, *La legislazione anti-terrorismo negli Stati Uniti:* inter arma silent leges*?*, in *Riv. it. dir. proc. pen*., 2005, 739.

[2] Un importante esempio in tal senso è costituito dalla sorveglianza su larga scala posta in essere dalla *National Security Agency* (NSA) statunitense sulle comunicazioni telefoniche, in base al c.d. FISA Act (*Foreign Intelligence Surveillance Act*) durante l'amministrazione Bush, e, a quanto pare, anche durante l'amministrazione Obama, nel 2013. In questa seconda ipotesi sembra che la sorveglianza di massa non abbia riguardato il contenuto delle conversazioni, ma i dati esterni (c.d. *metadata*) di tutte le comunicazioni intercorse (tramite il gestore Verizon) tra gli Stati Uniti e l'estero. Cfr. *https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order*.

"potenziale terrorista" o dal diverso soggetto posto sotto sorveglianza (il c.d. *target*). Di grande utilità sono naturalmente anche le variegate forme di controllo (*ex post* o in tempo reale) sulle innumerevoli attività che si svolgono nella rete (ivi compreso il controllo sulle transazioni finanziarie), nonché la *surveillance* sulle tradizionali attività di comunicazione, realizzate mediante dispositivi telefonici.

Le indagini informatiche, come vedremo, danno luogo a particolari problemi. Per l'ambiente in cui si svolgono esse hanno ad oggetto il dato digitale, caratterizzato da immaterialità, fragilità e ubiquità[3]; insistono su strumenti come la rete, server, o altri dispositivi informatici/elettronici, all'interno dei quali il dato può essere raccolto sia nella sua dimensione dinamica (cioè mentre fluisce), sia nella sua dimensione statica (cioè in quanto conservato nella memoria di server pubblici o privati, o in dispositivi elettronici ormai entrati nella nostra vita quotidiana, come *computer* oppure *netbook*, *tablet*, *smartphone* e analoghi dispositivi per la mobilità)[4]. Il che non rende sempre agevole distinguere (e qualificare giuridicamente) le attività di indagine, per individuare il relativo regime. Per non dire poi delle incertezze che si riscontrano in relazione alla posizione dei *Service Providers* e delle aziende costruttrici di *mobile devices*: fino a che punto sono tenuti a collaborare con l'autorità[5]?

[3] V. ad esempio, G. ZICCARDI, *Scienze forensi e tecnologie informatiche*, in L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2014, 4.

[4] Sul punto, sia consentito rinviare a G. DI PAOLO, voce *Prova informatica (diritto processuale penale)*, in *Enc. Dir.*, *Annali*, vol. VI, Milano, 2013, 736-762.

[5] Emblematica di tale difficoltà è stata la disputa tra FBI e *Apple*, insorta lo scorso febbraio 2016, allorché un giudice federale ha stabilito che l'azienda statunitense avrebbe dovuto aiutare l'FBI a sbloccare il telefono usato da Syed Rizwan Farook, l'uomo che ha ucciso 14 persone in una sparatoria il 2 dicembre a San Bernardino, in California (cfr. *http://www.internazionale.it/notizie/2016/03/29/fbi-apple-san-bernardino*, 29 marzo 2016). Altrettanto significativa è la vicenda che ha portato all'arresto, in Brasile, del capo di *Facebook*, per non aver fornito all'autorità giudiziaria procedente i dati di alcune chat di *WhatsApp* in un caso di narcotraffico. Non è chiaro se i dati fossero criptati, ma all'epoca *WhatsApp* ha dichiarato al New York Times che «non può fornire informazioni che non ha» (cfr. *www.theguardian.com*, 6 aprile 2016). Nel contesto dell'Unione europea, va infine menzionata la complessa e travagliata vicenda che ha riguardato il tema del *data retention* e la cessione dei dati personali a Paesi terzi (come gli Stati Uniti), che ha visto la Corte di giustizia annullare la direttiva in tema di *data*

Su un diverso piano, va rimarcato che l'enorme quantità di dati contenuti nelle memorie digitali, insieme al carattere "a-selettivo" degli strumenti di indagine, fanno emergere il rischio che una raccolta massiva e indiscriminata di dati possa mettere a repentaglio le libertà civili tradizionali, nonché i diritti fondamentali di nuova generazione (diritto alla *privacy*, diritto alla protezione dei dati personali, diritto alla garanzia della segretezza e integrità dei sistemi informatici).

Infine, rimane da evidenziare un ultimo aspetto problematico. Si allude al fatto che sempre più spesso, nello sconfinato mondo del *Web*, del *cloud computing* e delle telecomunicazioni, le attività di ricerca e raccolta delle "evidenze elettroniche" travalicano i confini nazionali, perché riguardano comunicazioni telematiche su utenze straniere o sistemi informatici o *providers* situati all'estero[6]. Vengono così in rilievo i limiti e le difficoltà che contraddistinguono i tradizionali meccanismi di cooperazione giudiziaria internazionale in materia penale, e la necessità di un adeguamento delle fonti internazionali e sovranazionali che si occupano della materia, tanto nell'ambito "piccola Europa", quanto nei rapporti con Paesi terzi.

Sono queste alcune delle principali declinazioni del diritto penale processuale della modernità.

---

*retention*, per difetto di proporzionalità (Corte di giustizia, 8 aprile 2014, cause riunite C-293/12 e C-594/12), dichiarare illegittimo l'accordo tra Unione europea e Stati Uniti (il c.d. accordo di *Safe Harbor*) che consentiva alle imprese americane (*Facebook* e *Google* principalmente, ma non solo) di conservare i dati degli utenti europei sia nella UE che negli USA (Corte di giustizia, 6 ottobre 2015, C-362/14); in precedenza, la Corte di giustizia aveva annullato anche l'accordo tra Unione europea e Stati Uniti avente ad oggetto il trasferimento dei dati personali dei passeggeri degli aerei diretti negli Stati Uniti (PNR) (Corte di giustizia, 30 maggio 2006, cause riunite C-317/04 e C-318/04). Di recente v. anche Corte di giustizia, 21 dicembre 2016, Tele2 e Watson, cause riunite C-203/15 e C-698/15.

[6] Cfr. A. MARLETTA, M. SIMONATO, *Le sfide della cooperazione internazionale nell'era digitale*, in *Cass. pen*., 2016, 1235 ss.

# COUNTERTERRORISM: NET WIDENING AND FUNCTION CREEP IN CRIMINAL JUSTICE

*John A.E. Vervaele*

SUMMARY: *1. Internationalization/globalization/integration and criminal justice in the post-industrial information society. 2. Transformation of the criminal justice system. 3. Redefinition of players (Authorities). 4. Redefinition of their competences and their techniques (the Sword). 5. Redefining the safeguards and the constitutional and human rights dimension (the Shield). 6. Consequences for the architecture (checks and balances, trias politica, constitutional dimension). 7. Constitutional and human rights standards: striking the right balance between justice and security? 8. Conclusion.*

## *1. Internationalization/globalization/integration and criminal justice in the post-industrial information society*

The internationalization of criminal justice is not new, in particular where internationalization is defined as a process of increasing cooperation between States and where States are influenced or controlled by international organizations. International public law conventions that prescribe binding substantive criminal law rules have been in existence for a century now, although their number and their impact have increased significantly. What is new is, I would say, twofold. Firstly, in the field of criminal justice, international organizations, such as the UN, the Council of Europe, the OECD and the FATF are monitoring the compliance process with international obligations, mostly through very detailed and politically binding evaluation mechanisms. We can find clear examples in the field of money laundering, corruption and terrorism. Secondly, international organizations as the UN Security Council or the international human rights courts are imposing international obligations upon Member States in criminal matters, without any specific conventional source and, thus, bypassing the signature and ratification process. In the aftermath of 9/11, the Security Council made the con-

ventional UN *acquis* in terrorism matters binding, regardless of signature or ratification by Party States. International human rights courts are moving towards prescription of offences, solely based on customary law and *ius cogens*, when it comes to serious human rights violations. Furthermore, international human rights courts are imposing far-reaching positive obligations upon States to protect human rights, including mandatory duties to investigate, to prosecute and to punish crimes.

The globalization of society is considerably more recent than the process of internationalization. Since the 1970s there has been a significant increase of standardization and unification of social processes (i.a. economic and cultural) by which they have become global. The idea of a global city[1] is the result of this process of internationalization. The globalizing society is based upon a worldwide increasing mobility of persons, goods, services and capital. Globalization of criminal justice is exceptional. However, the development of international criminal law and the establishment of international criminal courts, especially the ICC, can be considered as a very good example of dealing with globalized standards and institutions for the prosecution of war crimes and crimes against humanity and, in fact, also for dealing with justice and peace in situations of transnational justice.

Integration is a post-World War II phenomenon, by which policies of Member States are combined to form a whole (in Latin, *integer* means whole or entire). In other words, regional integration aims at common policies in a common area. This integration process is regional and goes hand in hand with the creation of supranational regional bodies, producing integration law and providing for regional adjudication in integration matters by a supranational Court of Justice. The integration process under the European Communities and since the Treaty of Maastricht under the European Union is a clear example. Quite unique in Europe[2] is the integration of justice matters, including criminal justice matters, in this process.

[1] S. SASSEN, *The global city: New York, London, Tokyo*, Princeton, updated 2nd edition, 2001.

[2] J.A.E. VERVAELE, *Mercosur and regional integration in South America*, in *International and Comparative Law Quarterly*, vol. 54, 2005, 387-410.

These processes of internationalization, globalization and integration in our societies have been combined in the past decades with the transformation of our societies into post-industrial information societies. The e-society or online society has completely reshaped social behaviour and social structure. A single information society concept does not exist. Scientists are struggling about definitions and values of the concept and focus on economic, technical, sociological and cultural patterns. Postmodern society is often characterized as an «information society», because of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society indeed emphasizes the technological innovation. Information processing, storage and transmission have led to the application of information and communication technology (ICT), and related biotechnology and nanotechnology, in virtually all corners of society. The information society is a post-industrial society in which information and knowledge are key-resources and are playing a pivotal role[3].

However, information societies are not solely defined by the technological infrastructure in place, but rather as multidimensional phenomena. Any information society is a complex web, not only of technological infrastructure, but also as an economic structure, a pattern of social relations, organizational patterns, and other facets of social organization. Therefore, it is important to focus not only on the technological side, but also on the social attributes of the information society, which include the social impact of the information revolution on social organizations, such as the criminal justice system.

Moreover, the postmodern age of information technology transforms the content, accessibility and utilization of information and knowledge in the social organizations, including the criminal justice system. The relationship between knowledge and order has fundamentally changed. The transformation of communications into instantaneous information-making technology has changed the way society values knowledge. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control.

[3] D. BELL, *The Coming of Post-Industrial Society*, New York, 1976.

The emergence of a new technological paradigm based on ICT has resulted in a network society[4], in which the key social structures and activities are organized around electronically processed information networks. There is an even deeper transformation of political institutions in the network society: the rise of a new form of State (network-State) that gradually replaces the nation-States of the industrial era. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control (surveillance society). The transition from the nation-State to the network-State is an organizational and political process prompted by the transformation of political management, representation and domination in the conditions of the network society. All these transformations require the diffusion of interactive, multi-layered networking as the organizational form of the public sector. Information and knowledge are key-resources of the information society, affecting the social and political structure of society and State and affecting the function, structure and content of the criminal justice system.

## *2. Transformation of the criminal justice system*

What is the impact of these developments on the domestic criminal justice system? It is quite clear that the domestic criminal justice system has not been replaced by a global one, in the global city. Societal globalization does not automatically lead to legal globalization or globalization of criminal justice and not even to globalization of political authority with regard to criminal justice. The birth of international criminal law adjudication is the exception and is the outcome of a process that has been going on for a century. Even though in place, this new system of justice is still building up its own concepts of criminal law and criminal procedure. However, the process of internationalization and globalization, both offline and online, does affect the domestic criminal justice system substantially. Domestic criminal justice is faced with socie-

[4] M. CASTELLS, *The Rise of the Network Society. The Information Age: Economy, Society and Culture. Volume 1*, Malden, Second Edition, 2000.

tal changes by which perpetrators are committing crimes and by which the crime, the perpetrators themselves and, *inter alia*, evidence are not always linked with the territory of the nation-State. As a consequence of the increasing mobility of persons, goods, services and capital, the domestic criminal justice systems have to protect new legal interests (*Rechtsgüter*), which usually have a strong transnational background (for example, protection against hate speech and xenophobia, protection against child pornography or protection against securities fraud or against ID theft). The domestic criminal justice system is internationalizing in a process of top-down internationalization and bottom-up internationalization. International and regional organizations are imposing new substantial and procedural obligations upon domestic criminal justice systems, but the domestic criminal justice systems are also increasing their international dimension in order to deal with criminality in a globalizing society. This means that the domestic criminal justice system is both at the user and the supply side of this process.

However, this renewal is not limited to some updating of offences based upon new or renewed legal interests to protect, nor limited to an increase of mutual legal assistance. In fact, the classical rationale for the use of criminal justice (starting with the primary criminalization by the definition of offences) – based upon *ultimum remedium*, strict conditions of harmful conduct that violates legally protected interests and concepts derived from the Enlightenment and Kantian philosophy – has been replaced in the past decades by a globalizing criminal policy concept, translated into criminal policy paradigms: combat/war against drugs, combat/war against organized crime, combat/ war against terrorism. I call them paradigms, because they function as a frame of reference for the perception of reality and thus for the definition of social constructs as crime, danger, risk and insecurity. These criminal policy paradigms have been used both at the domestic and at the international level in order to justify substantial changes in the relation between State-society and criminal justice and in the criminal justice system itself.

Modern criminal justice, with its roots in the Enlightenment, provides for an integrated system, offering both *protection* to individuals (not only suspects) (the shield dimension), *instruments* for the law en-

forcement community made up of the police, the Public Prosecutor's Office and the judiciary (the sword dimension), and providing for *checks and balances/trias politica* (the constitutional dimension). As mentioned, three paradigms, the combat/war on drugs, the combat/war on organized crime and the combat/war on terrorism swept like a tidal wave through the criminal justice system. All three dimensions of the criminal justice system have been affected by these three waves. These paradigms have transformed our criminal justice systems in its entirety, affecting general criminal law, special criminal law, criminal procedure and international criminal law. In 1999 the International Association of Penal Law (AIDP-IAPL) presented an excellent analysis of this transformation under the title *The Criminal Justice Systems Facing the Challenges of Organized Crime*[5].

There is no doubt that substantial and far-reaching changes have also occurred during the last decade. The new security paradigm and counterterrorism policy have resulted in transformations that go far beyond the field of terrorist offences. International pressure for a common approach to terrorist investigation, prosecution and judgment has been intense. Both at the UN and at the Council of Europe, an impressive set of international and regional Conventions have been elaborated on Organized Crime and Counterterrorism. After 9/11, the UN paved the way with Security Council resolutions and the establishment of a Counter-Terrorism Committee that is supervising the implementation of the resolutions, including the substance of the conventions[6]. The third wave of reforms of counterterrorism has evolved before the 9/11 events and the events in Madrid and London, but has certainly been intensified by these terrorist attacks.

Although there has been a substantial paradigm shift (from drugs to organized crime and to terrorism), the three paradigms have transformed, through a common and cumulative security-orientated approach, the objectives, nature and instruments of the criminal justice system. The objective of the criminal justice system has changed from

[5] See the Reports by T. WEIGEND, C. BLAKESLEY, J. PRADEL, C. VAN DEN WYNGAERT, in *International Review of Penal Law*, 1996, 527-638.

[6] See *www.un.org/sc/ctc/countryreports/reportA.shtml* for the comprehensive national reports.

punishment of guilty perpetrators of committed offences (with general and special preventive aims, including rehabilitation) towards a broader field of social control of danger and risk[7].

Based on these paradigms, general criminal law and special criminal law have been widened in order to include preparatory acts and incrimination of criminal organizations and terrorist organizations (or conspiracy variants of it). As a result, the commission of criminal conduct by a suspect is no longer the triggering threshold for the *ius puniendi* of the State. The threat of organized crime or terrorist crime by setting up organizations (with a very low threshold definition) is sufficient for criminalization. The criminalization of apology of terrorism or other apologies (xenophobia) demonstrates a similar trend. Such offenses concern the criminalization of the mind (and may touch upon the freedom of expression) of a person, instead of the criminalization of a criminal act, based upon conduct. By redefining the objective of criminal justice, its very nature has been converted. The greater the risk or the danger, which is based on a social construction and certainly not on empirical facts, the lower the threshold for using the *ius puniendi*, which means that criminal law turns into security law. Security law is not so much based on a legal definition of suspect and criminal conduct, linked to serious harm to a legal interest, but is based upon a preset definition of an enemy[8] that is associated with risk, danger and insecurity. The security approach in criminal law has led to an expansion of substantive criminal law (general part and special part) beyond the traditional boundaries and limits as defined by the Enlightenment. This raises the question whether harmonization or the mandatory criminalization of offences under international and regional European law

[7] In continental theories of criminal law, a basic distinction is made between the effects of punishment on the man being punished – individual prevention or special prevention – and the effects of punishment upon the members of society in general – general prevention. The characteristics of special prevention are termed «deterrence», «reformation» and «incapacitation». General prevention, on the other hand, may be described as the restraining influences emanating from the criminal law and the legal machinery. See: J. ANDENAES, *General Preventive Effects of Punishment*, in *University of Pennsylvania Law Review*, 114, 1965-66, 949-983.

[8] G. JAKOBS, *Bürgerstrafrecht und Feindstrafrecht*, in *HRRS*, III, 2004, 88-95.

should not be combined with the harmonization of obligations of general criminal law. The precise impact of the harmonization and mandatory criminalization could then be defined and, in addition, it could be avoided that the top-down internationalization and regionalization ends up in an atrophy of punitivism or penal inflation. If the international community and European community are acting as legislators, which concepts of *nulla poena sine culpa* and of criminal liability do they use?

The transformation of the criminal justice system, especially in the era of counter-terrorism (third wave), has had even more far-reaching consequences, especially for the field of criminal procedure[9], and has affected:

- the type of players/authorities;
- their powers and investigation techniques (including digital) – the sword dimension;
- the safeguards and constitutional and human rights to be respected – the shield dimension;
- the architecture (checks and balances, trias politica) – the constitutional dimension.

### *3. Redefinition of players (Authorities)*

In the first place, traditionally, criminal investigation has been supervised by judicial authorities and coercive measures are authorized and/or are executed by members of the judiciary (investigating judges or pre-trial judges or trial judges). In many countries we can see a shift in the pre-trial phase from judicial investigation to prosecutorial and police investigation. We can clearly speak of a reshuffling of responsibilities in the law enforcement community. Magistrates are less and less involved in the pre-trial phase as such; there is a clear shift to the executive or to semi-executive branches of State power.

[9] For a more elaborated version, see J.A.E. VERVAELE, *Special procedural measures and respect of human rights, general report for the International Association of Criminal Law* (AIDP), in *Utrecht Law Review*, 2009, 66-109.

Secondly, there is not only a shift between the classic players; new players, such as administrative enforcement agencies, also play an increasing role in the field of fighting serious crime. The intelligence community is gaining ground in the criminal justice system, both as specialized police units dealing with police intelligence and as security agencies. These intelligence entities are responsible as the forerunners of police and intelligence-led investigations, and in some countries they have even obtained coercive and/or judicial competence. Furthermore, classic law enforcement agencies convert into intelligence agencies and change their culture and behaviour. Thirdly, many countries have increased the use of private service providers (telecom, business operators, financial service providers) and professions with information privileges (such as lawyers and journalists) as gatekeepers and as the long-arm collectors of enforcement information. Journalistic and legal privileges are no longer safe havens.

*4. Redefinition of their competences and their techniques (the Sword)*

Firstly, in most countries the paradigms of the drugs-trade, organized crime and terrorism are not only used to redefine investigative, coercive instruments, but also to introduce new special investigative techniques, such as wiretapping, infiltration and observation, which can only be applied to investigate serious crimes. The result is a set of coercive measures with a double use (for serious and less serious offences) and a set of coercive measures with a single use for certain serious crimes.

Secondly, in many countries the classic measures dealing with securing evidence and the confiscation of dangerous instruments or products in relation to crime have become an autonomous field of security measures concerning goods and persons (e.g. seizure and confiscation, detention orders and security orders). Related to that, investigations into the financial flows from the drugs trade, organized crime (financing, money laundering) and terrorism (financing) have been converted from a classic investigation for gathering evidence into an autonomous financial investigation, dealing with extensive seizure and confiscation of

the proceeds of crime (asset recovery) and/or into autonomous financial surveillance and investigations into the financing of serious crime.

Thirdly, the triggering mechanisms or minimum thresholds for the use of coercive measures to combat serious crimes are changing. Criminal investigation no longer starts with a reasonable suspicion that a crime or an offence has been committed or attempted, or with a reasonable suspicion that a preparatory act for committing a serious crime has been committed or attempted. Investigative techniques and coercive measures are also used in a proactive or anticipative way to investigate, *anti-delictum*, the existence and behaviour of potentially dangerous persons and organizations in order to prevent serious crimes. This proactive criminal investigation includes the situation in which there is not yet any reasonable suspicion that a crime has been committed, is about to be committed or that specific preparatory acts have taken place and in which, of course, there can be no suspect(s) legally speaking. The objective of proactive investigations is to reveal the organizational aspects in order to prevent the preparation or commission of a serious crime and to enable the initiation of criminal investigation against the organization and/or its members. This use of coercive measures for crime prevention can be realised by intelligence agencies, police authorities or judicial authorities. When doing so, they belong to the intelligence community, even if they are normally authorities belonging to the law enforcement community. In that time frame they might collect information and use certain coercive measures of criminal procedure in order to prevent the preparation or commission of the crime. In this area of criminal law without suspects we see a new combination of proactive or anticipative enforcement and coercive investigation (*Vorbeugende Verbrechensbekämpfung*, *Vorfeldaufklärung* and *Vorermittlung*). The conversion from a reactive punishment of crime into a proactive prevention of crime has far-reaching consequences. The distinction between police investigation and judicial investigation is under pressure. Coercive proactive enforcement becomes important for serious crimes. The intelligence community becomes a main actor in the law enforcement field. Preventive criminal law is not about suspects and suspicion, but about information gathering (information and criminal intelligence investigation) and procedures of exclusion against potentially danger-

ous persons. The criminal justice system is increasingly used as an instrument to regulate the present and the future and not to punish for behaviour in the past, and the criminal process is becoming a procedure in which the pre-trial investigation is not about truth-finding related to committed crime, but about construction and de-construction of social dangerousness.

Fourthly, the sword of criminal justice has changed substantially through the use of digital-led investigation (online criminal searches, the monitoring of data flow, data processing) and the use of advanced technology in judicial investigations (digital surveillance, detection devices, etc.). Information-led investigation replaces mere suspicions. The expansion of the judicial investigation into a proactive investigation and the increasing overlap between the law enforcement community and the intelligence community has been further increased by the technological developments in investigative devices: the sword of technology with far-reaching eyes and razor-sharp edges. Thanks to new technology, the methods of surveillance for communication, the physical surveillance of persons and their movements and activities and for transactional surveillance (of their services) have changed dramatically. Technology has completely changed not only the behaviour of citizens, but also, through the use of wiretapping, video surveillance, tracking devices, detection devices and see-through devices, data mining, remote digital searches, Trojan horses, and so forth, the environment of enforcement and proactive enforcement.

### *5. Redefining the safeguards and the constitutional and human rights dimension (the Shield)*

In many countries, the legislator considered some procedural guarantees as burdens to the efficiency of serious crime prevention, serious crime investigation and serious crime prosecution. First of all, the use of existing instruments such as search and seizure and police detention is submitted to other parameters for serious offences than for less serious offences. Moreover, judicial authorization (in the form of warrants) is weakened or abolished for some coercive measures (warrantless co-

ercive measures). The role of the defence and of the judge as procedural guarantees is reduced. This means in practice that the police and prosecutors have more autonomy and are subjected to diminished supervision by the judiciary on their investigative work. We could speak of a two-fold expansion of the existing coercive measures: a general expansion of the powers of the police and prosecutors with relaxed safeguards, which trend is even stronger for the investigation of serious crimes because of the presence of a security interest. Generally speaking, we can say that the seriousness of the crimes under the aforementioned paradigms is used to justify raising the sword and lowering the shield. In many countries, in the case of serious crimes, the relationship between the intrusiveness of the measures and judicial control has changed: the greater the security interest, the less the judicial control and the procedural safeguards.

Secondly, by lowering the thresholds (reasonable suspicion or serious indications to simple indications, reversed burden of proof, legal presumptions of guilt) for triggering the criminal investigation and for imposing coercive measures, the presumption of innocence is undermined and replaced by objective security measures. The shields protecting the citizen against the *ius puniendi* of the State are put at the back of the stage in the theatre of criminal justice. This has, of course, direct consequences for habeas corpus, habeas data, fair trial rights, redefinition of evidence rules, public proceedings, etcetera.

In the third place, in many countries there is also a need to secure the functioning of the criminal justice system and its players. The protection of witnesses has also been converted into the protection of anonymous witnesses, including those from the police authorities and intelligence agencies involved in infiltration. The criminal justice system is increasingly shielding its agents against the defence through *ex parte* proceedings, forms of secret evidence-gathering and the use of secret evidence in the pre-trial and trial setting.

Fourthly, several countries have amended their mandate for intelligence forces and their powers. Their investigative competences now include coercive powers, parallel to the ones in the Code of Criminal procedure, and their objective also includes the prevention of serious crime, as this constitutes a threat to national security. In some countries

they need the authorisation for the use of these powers by a public prosecutor or by the executive branch of government. *De facto*, the intelligence community is using judicial coercive powers without being a judicial authority and without the guarantees of some form of judicial warrant and/or judicial supervision. We can see an overlapping competence between the intelligence agencies and the police authorities acting as intelligence community in the preliminary proactive or anticipative investigation.

In the fifth place, we see an increasing use of intelligence in the criminal justice system. As long as it is used as steering information or as data sharing or as triggering information for the opening of a judicial investigation it does not affect or infect the criminal justice system. However, when intelligence is used as triggering information, establishing probable cause for using coercive measures, or as evidence in criminal proceedings it does infect the classic rules of fair trial and equality of arms, as most of this type of intelligence can only be used in shielded and secret *in camera* and *ex parte* proceedings. This is even the case in international criminal justice.

It goes without saying that all these transformations affect the position of the defence lawyer in the criminal process. His legal privilege is under pressure. In certain countries, when dealing with secret evidence in cases of organized crime and terrorism, the defence lawyer has no full access to the file (limited disclosure) or only special security screened bar lawyers can act on behalf of the suspect. The defence lawyer's role and his duties and responsibilities are redefined.

### *6. Consequences for the architecture (checks and balances, trias politica, constitutional dimension)*

The reforms result in a clear expansion of the punitive State[10], thereby disfavouring the Rule of Law. The focus on public security and preventive coercive investigation is clearly undermining the criminal

[10] N.A. FROST, *The Punitive State: Crime, Punishment and Imprisonment across the United States*, New York, 2006.

justice system and its balances between the sword and the shield. Administrative and preventive forms of punitive justice are expanding. The result is also that the equilibrium between the three branches of the trias politica is under great pressure in favour of the executive.

In the majority of European countries transformations have resulted in a distinction within the ordinary criminal justice system between a criminal procedural regime for serious offences and one for «petty» offences or in special legislation replacing substantial parts of the ordinary criminal justice system. In fact, criminal procedure is no longer organized in line with the general part of criminal law, but in line with the dual use in the special part of criminal law. The exceptional features for organized crime and terrorism changed from the exception into the main and common procedure for serious crimes, for which reason we can speak of the normalization of the exception.

### *7. Constitutional and human rights standards: striking the right balance between justice and security?*

The three paradigms of criminal policy, based on a security approach have not only resulted in neo-punitivism but also in shifts in the criminal justice systems that undermine the basic concepts of the *ius puniendi* under the rule of law.

Although the criminal justice reforms have detached the criminal justice systems from some of its own fundamental values, at the same time, in the last decade, we can see in several countries an increasing process of constitutionalisation of criminal justice matters, both in law (including constitutional norms concerning the rule of law and fair trial) and in practice (by the case law of the higher courts and the supranational human rights courts). Special criminal procedures dealing with organized crime and counterterrorism are dealt with by Supreme Courts, Constitutional Courts and human rights Courts.

I am not convinced that this process is an intrinsic outcome of the criminal justice reforms themselves. It is true that in many countries reforms were introduced in favour of adversarial proceedings, based on accusatorial principles, such as immediacy, equality of arms, fair trial,

an independent and impartial judiciary. However, at the same time, parallel reforms have been introduced to reduce the scope and application of these principles when investigating, prosecuting and adjudicating serious offences.

Although the constitutional and human rights standards have become a mandatory framework for dealing with the effect in law and law in practice of these paradigms of crime, the panorama is, for the moment, rather a patchwork. The European Court of Human Rights has given a very broad margin of appreciation to the Member States when it comes to criminal justice and terrorism, certainly related issues such as fair trial, rights of the defence, protection of the privacy and freedom of expression. It took a tougher stand when it comes to inhuman treatment and torture. However, the European Court of Justice has imposed a high human rights standard in the area of blacklisting of terrorists and terrorist organizations. Nevertheless, this field is, of course, not representative for the classical field of procedural safeguards in criminal matters (a field in which the EU legislator has great difficulty to define common standards that do not violate the minimum denominator of the ECHR case law). Also at the level of the national Supreme and Constitutional Courts, we see an increasing case-load concerning important aspects of the basic concepts of criminal justice. However, as it stands, we cannot say that these Courts are producing common standards. Just to take two examples: the case law of these Courts on special investigative techniques and the use of secret evidence is quite diverging as is their case law on the digital investigative techniques and even on data retention by service providers.

## *8. Conclusion*

We are living in a time in which many reforms of the criminal justice system are the result of a political instrumentalisation and mediatisation of crime and the fear of crime. These reforms are being justified by the criminal policy paradigms of combating drugs, organized crime and terrorism. The result is that the *ius puniendi* of the State (being one of the most repressive interferences in liberty on behalf of the State), is

being instrumentalised and put at service of danger and risk management. When prevention of dangerousness becomes the triggering mechanism for the use of very intrusive investigative techniques and criminal punishment, the criminal justice system is risking perverting into a security system. These developments result in a substantial expansion of the criminal justice system, through substantive and procedural criminal law, and thus of expanded interference with the liberty of citizens. The expansion of criminal justice goes hand in hand with the erosion of its basic principles (*nullum crimen sine iniuria*, *nulla poena sine culpa*, *ultimum remedium*, fair trial, etcetera). At the same time, criminal repression becomes a «passe-partout» formula for solving societal problems. The expectations about the problem-solving capacity of criminal justice are however in sharp contrast with the real performance. The expansion of criminal justice is very real in terms of social control, but very symbolic in terms of societal problem solving capacity.

The criminal policy paradigms (drugs, organized crime, and terrorism) are used as political justifications at the domestic, European and International level. We can certainly not conclude that the European and/or international dimension have unilaterally caused these shifts. The three levels are strongly interacting under the same paradigms. Nevertheless it is useful to have a closer look at the new international and European dimension. At first sight we could believe that the international criminal justice, dealing with war crimes and crimes against humanity, is a clear example of victory of justice over insecurity, as it is the expression of the international community to deal at a global level with the most severe violations of human rights. Global criminal justice as reaction against impunity is of course a noble ideal. At second sight, we see, however, that also international criminal justice is struggling with some of the same problems (mediatisation, political discretion for the prosecutor, symbolic function, etcetera). The international criminal justice system in action has also to deal with problems and shifts of responsibilities common to the domestic criminal justice system. To illustrate this, I refer to the definition of joint criminal enterprise, a form of organized criminal acting and the problems with the *nullum crimen sine lege* rule in international criminal justice, or the use of secret evidence and limited disclosure in international criminal justice. The European

dimension is a complete different one, as the integration model of criminal justice is limited to rule setting and in the future maybe to some supranational investigative tools, but the criminal adjudication continues to be the full competence of the Member States. Nevertheless the EU itself has been struggling in its criminal policy plans with striking the right balance between security and liberty. The EU Court of Justice has a good record when it comes to constitutional standards and human rights protection in the EU, but the criminal law legislation of the EU is rather running to the bottom of the lowest denominator. Recent legislative action to harmonize procedural safeguards in the framework of the mutual recognition instruments (such as the European arrest warrant and the European evidence warrant), dealing with the right to a lawyer, the right to translation, a letter of rights, etcetera have been accompanied with great reluctance from many Member States to agree upon equivalent common standards. Meanwhile the European Court of Justice had to elaborate human rights for the integrated area, such as the application of the transnational *ne bis in idem* principle[11] or the protection of the right to privacy[12]. The opportunities and threats of European integration in criminal matters should be highlighted. The new Lisbon Treaty offers the necessary political and legal tools to strike a right balance between liberty and security, between effective criminal law enforcement and procedural safeguards. To reach a good result, it will, however, be necessary that Member States are willing to further integrate their criminal justice systems. This includes the setting of equivalent standards and steering of their administration of justice, also in the sensitive area of counterterrorism.

[11] J.A.E. VERVAELE, *Schengen and Charter related* ne bis in idem *protection in the Area of Freedom, Security and Justice: M and Zoran Spasic*, in *Common Market Law Review*, 52, 2015, 1339-1360; ID., *Ne Bis In Idem: Towards a Transnational Constitutional Principle in the EU?*, in S. GLESS, J.A.E. VERVAELE (eds.), *Special on transnational criminal justice*, in *Utrecht Law Review*, 2013, 211-229.

[12] Case C-392/12, Digital Rights Ireland, ECJ Judgment of 16.05.2014 and Case C-362/14, Schrems (Safe Harbour), ECJ Judgment of 06.10.2015.

# LE INDAGINI INFORMATICHE CONTRO IL TERRORISMO

## BILANCIAMENTI DIFFICILI E TIMORI LEGISLATIVI

*Marcello Daniele*

SOMMARIO: *1. Una coppia indissolubile. 2. Il diritto alla riservatezza in pericolo. 3. Le indagini informatiche non occulte: l'*upgrading *dei tradizionali mezzi di ricerca delle prove fisiche. 4. Le indagini informatiche occulte. 4.1. Le intercettazioni ubique. 4.2. Le videoriprese come* panopticon*. 4.3. Le perquisizioni* on-line *e un'auspicabile ibridazione degli strumenti repressivi e preventivi. 5. I pericoli dell'inerzia legislativa.*

### *1. Una coppia indissolubile*

Il terrorismo e le indagini informatiche rappresentano una coppia indissolubile nell'era della globalizzazione. Si evolvono di pari passo. Più il terrorismo, grazie alle tecnologie digitali e all'uso delle reti informatiche, espande la sua capacità di reclutamento e la sua forza letale, più, parallelamente, le indagini informatiche si raffinano e ampliano la loro valenza repressiva.

Mirando a rafforzare le seconde per contrastare il primo, il legislatore si trova alle prese con un difficile contemperamento fra i valori in gioco. Qualunque soluzione rischia di sacrificare in modo eccessivo le esigenze repressive o, al contrario, i diritti fondamentali dell'accusato e delle altre persone coinvolte nei procedimenti penali. Ma è una sfida a cui i *conditores* non possono sottrarsi. Non vi sarebbe nulla di peggio che eluderla, rinunciando ad introdurre regole in linea con gli sviluppi tecnologici, e lasciando alla giurisprudenza il compito di riempire tale vuoto con i propri bilanciamenti.

## *2. Il diritto alla riservatezza in pericolo*

Le indagini informatiche sono fra le più insidiose che si conoscano soprattutto a causa del loro esteso raggio operativo. Non riguardano luoghi, persone o oggetti fisici ben delimitati, come le tradizionali ispezioni, perquisizioni e sequestri. Né si limitano a carpire singoli flussi di comunicazioni, come le intercettazioni. Possono coinvolgere enormi luoghi virtuali, pieni di informazioni di ogni genere relative alla vita delle persone; magari racchiusi in piccoli dispositivi elettronici, oppure fisicamente impalpabili ma agevolmente raggiungibili, come le reti informatiche. Luoghi che possono venire approfonditamente sondati da chi le svolge, con un'inevitabile limitazione del diritto fondamentale alla riservatezza previsto dagli artt. 14 e 15 Cost., 8 CEDU e 7 e 8 CDFUE[1].

La Corte europea dei diritti dell'uomo ha da tempo individuato i requisiti minimali che le norme restrittive della *privacy* finalizzate alla prevenzione e alla repressione dei reati dovrebbero presentare: un'adeguata base legale, attraverso la previsione di regole accessibili, prevedibili nel loro esito applicativo e sufficientemente precise; nonché, in osservanza del generale canone di proporzionalità che si trova alla base dei bilanciamenti[2], il rispetto del contenuto essenziale del diritto, mediante la previsione di adeguate garanzie processuali volte a compensarne la compressione[3].

Il livello di interferenza con la riservatezza varia secondo la tipologia di indagine effettuata. A questo proposito è opportuno prendere le

[1] Intendiamo qui il diritto alla riservatezza come un diritto capace di ricomprendere non solo oggetti fisici (i luoghi privati, la corrispondenza), ma qualunque luogo, anche virtuale, in rapporto a cui sia consentito vantare uno *ius excludendi* (si pensi al c.d. domicilio informatico). V. al riguardo R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, 1152 s., e L. PICOTTI, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *www.archiviopenale.it*, 2016, n. 2, 5 s.

[2] In particolare rinvenibile nella clausola della «necessità in una società democratica» prevista dall'art. 8 § 2 CEDU.

[3] V., fra le molte, Corte eur. dir. uomo, Grande Camera, 4 dicembre 2015, *Roman Zakharov c. Russia*, § 163 s.

mosse da una distinzione: quella fra indagini informatiche "non occulte" e "occulte".

### *3. Le indagini informatiche non occulte: l'*upgrading *dei tradizionali mezzi di ricerca delle prove fisiche*

Le indagini informatiche "non occulte" sono quelle che avvengono con la percezione delle persone che vi sono sottoposte. Considerata tale loro caratteristica, si tratta di indagini perlopiù finalizzate alla repressione, ossia per rinvenire nei dispositivi e nelle reti informatiche le prove digitali dei reati già commessi.

Esse sono state introdotte nel nostro sistema già con la l. 18 marzo 2008 n. 48, la quale, recependo la Convenzione di Budapest del 2001[4], ha appositamente modificato le norme del codice di procedura penale in tema di ispezioni, perquisizioni e sequestri[5].

Ne è risultata una disciplina che, nonostante presenti non pochi difetti[6], appare capace di preservare la *privacy* perlomeno nel suo nucleo essenziale. Le indagini vanno autorizzate o, comunque, convalidate dal pubblico ministero con un decreto motivato, con il diritto del difensore di assistervi e la possibilità di impugnare gli eventuali provvedimenti di sequestro di fronte al tribunale del riesame[7]. Dal canto suo l'indagato, in applicazione della garanzia del *nemo tenutur se detegere*, non è tenuto a rivelare agli organi inquirenti eventuali *password*, chiavi di crittografia o altre modalità di accesso ai dispositivi o ai sistemi informatici oggetto delle investigazioni[8].

---

[4] Ossia la Convenzione del Consiglio d'Europa sulla criminalità informatica, stipulata il 23 novembre 2001.

[5] V. al riguardo, anche sotto il profilo della possibilità di acquisire i messaggi di posta elettronica, F. ZACCHÈ, *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust*., 2013, n. 4, 106 s.

[6] Su cui cfr. G. DI PAOLO, *Prova informatica (diritto processuale penale)*, in *Enc. dir*., *Annali*, vol. VI, Milano, 2013, 756 s.

[7] Si vedano gli artt. 244, 247, 352 e 355, 257 e 324, 356 e 365 c.p.p.

[8] Cfr. L. LUPÁRIA, Computer crimes *e procedimento penale*, in G. GARUTI (a cura di), *Modelli differenziati di accertamento*, tomo I, Torino, 2011, 387. Resta ovviamente

Il rischio maggiore che queste indagini determinano riguarda perlopiù l'affidabilità cognitiva dei loro risultati[9]. Un obiettivo posto in pericolo dalla agevole modificabilità delle prove digitali, alterabili da parte di chiunque tenti di acquisirle senza utilizzare le dovute metodiche. Il legislatore ne è consapevole, fissando due essenziali direttive da osservare in rapporto a qualunque attività di raccolta delle prove digitali: *a*) l'impiego di «misure tecniche» in grado di «assicurare la conservazione» e di «impedire l'alterazione» dei dati originali[10], e *b*) la copia dei dati su «adeguati supporti», tramite tecniche che assicurino «la conformità della copia all'originale e la sua immodificabilità»[11].

Nessun obbligo, pertanto, di adottare specifiche modalità di raccolta, ma solo l'indicazione di obiettivi. Una scelta saggia, se si considera la rapida ed incessante evoluzione che contraddistingue l'informatica, ma che al contempo ha come conseguenza l'assenza di sanzioni. Non sono configurabili nullità o inutilizzabilità quando le indagini informatiche non sono svolte da esperti, o quando vengono impiegate tecniche che non risultano in grado di assicurare le finalità perseguite dal legislatore[12].

L'unico antidoto alla fallibilità delle indagini informatiche è costituito dal contraddittorio: il quale in questo caso si concretizza nella possibilità per la difesa di partecipare alla raccolta delle prove digitali con i propri consulenti, con la facoltà di questi ultimi di contrapporsi dialetticamente ai consulenti dell'accusa.

Sotto questo profilo la giurisprudenza incorre in un ricorrente errore concettuale: quello di includere queste indagini nella categoria degli

---

salva la possibilità per gli organi inquirenti di accedere ai sistemi informatici con mezzi propri, anche avvalendosi della collaborazione di privati.

[9] Si veda G. UBERTIS, *Argomenti di procedura penale*, vol. IV, Milano, 2016, 113 s.

[10] Art. 244 comma 2 c.p.p.; v. anche gli artt. 247 comma 1 *bis*, 254 comma 2, 259 comma 2, 352 comma 1 *bis* e 354 comma 2 c.p.p.

[11] Art. 260 comma 2 c.p.p.; v. anche gli artt. 254 *bis* e 354 comma 2 c.p.p.

[12] Si rinvia a M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, 294 s.; v. pure F. CAJANI, *Il vaglio dibattimentale della* digital evidence, in *Arch. pen.*, 2013, 837 s. In senso contrario cfr. F. GIUNCHEDI, *Le* malpractices *nella* digital forensics. *Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. pen.*, 2013, 828 s.; L. LUPÁRIA, Computer crimes, cit., 389 s.; L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, 4521 s.

accertamenti tecnici ripetibili, con la conseguente applicabilità delle prescrizioni dell'art. 359 c.p.p. Il che porta alla raccolta delle prove digitali ad opera del solo consulente dell'accusa, mentre alla difesa non resta altro che il contraddittorio posticipato esperibile attraverso l'esame incrociato del consulente dell'accusa in dibattimento[13].

È un'impostazione che non tiene conto della congenita modificabilità delle prove digitali. Qualunque ingresso in un sistema informatico rischia sempre di alterare i dati in esso contenuti, generando mutazioni che, anche se minimali, potrebbero risultare decisive[14].

Ciò suggerirebbe di applicare la procedura degli accertamenti tecnici non ripetibili *ex* art. 360 c.p.p.: il preavviso alla difesa in ordine al compimento delle operazioni, la possibilità di parteciparvi con un proprio esperto e il diritto all'impiego delle forme dell'incidente probatorio. Neppure questa soluzione sarebbe, però, ineccepibile. Non la si potrebbe adottare in tutte le situazioni in cui le indagini informatiche dovessero essere effettuate a sorpresa, evitando di porre l'indagato nelle condizioni di alterare le prove.

Di qui l'opportunità di un approccio pragmatico, graduando il contraddittorio sulla base della situazione concreta. Alla più garantita procedura dell'art. 360 c.p.p. si dovrebbe rinunciare, in particolare, nelle ipotesi in cui le indagini riguardassero dati tali da trovarsi nella potenziale disponibilità dell'indagato[15].

---

[13] V. ad esempio Cass., sez. I, 5 marzo 2009, n. 14511; più di recente, sez. II, 4 giugno 2015, n. 24998. In dottrina cfr. F.M. MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen*., 2013, 1264 s.

[14] Cfr. P. TONINI, *Considerazioni su diritto di difesa e prova scientifica*, in *www.archiviopenale.it*, 2011, n. 3, 11 s.

[15] Cfr. S. ATERNO, Digital forensics *(investigazioni informatiche)*, in *Dig. Disc. pen*., agg. VIII, Torino, 2014, 236 s.; E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen*., 2010, 1530 s.; L. MARAFIOTI, Digital evidence, cit., 4519 s.; A. TESTAGUZZA, Digital forensics. *Informatica giuridica e processo penale*, Padova, 2015, 46 s.; v. pure M. DANIELE, *La prova digitale*, cit., 297 s.

## *4. Le indagini informatiche occulte*

Ben più efficace contro il terrorismo si rivela un'altra categoria: quelle delle indagini "occulte", in quanto non percepite nel loro svolgimento da parte di chi vi è sottoposto. Indagini preziose non solo in chiave repressiva, ma anche e soprattutto in chiave preventiva, in quanto consentono una sorveglianza segreta e costante dei gruppi criminali.

È chiaro come esse incrementino i rischi per la riservatezza; specie se si tiene conto del fatto che le loro potenzialità applicative risultano notevolmente ampliate dagli sviluppi della tecnologia[16].

### *4.1. Le intercettazioni ubique*

Una prima tipologia è rappresentata dalle intercettazioni, le quali risultano particolarmente insidiose quando vengono svolte attraverso l'impiego dei c.d. *trojan* (o captatori informatici): vale a dire *virus* che, introdotti nei dispositivi (*smartphone*, *tablet*, *personal computer*) di determinate persone, consentono agli organi inquirenti di attivarne e controllarne a distanza il microfono, in modo da captare e registrare i suoni circostanti.

Si tratta di intercettazioni ambientali, nella sostanza, ubique, in quanto suscettibili di avvenire in qualsiasi luogo in cui il dispositivo intercettato si trovi. Naturalmente valgono anche per esse i requisiti previsti a pena di inutilizzabilità dall'art. 271 comma 1 c.p.p.; in particolare, il vaglio del giudice per le indagini preliminari sulla scorta dei parametri fissati dall'art. 267 c.p.p., e l'indicazione delle loro modalità

[16] Un'ulteriore forma di indagini occulte è rappresentata dal monitoraggio dei siti *internet* utilizzati dai potenziali terroristi, previsto dall'art. 2 commi 2 s. del d.l. 18 febbraio 2015, n. 7 (convertito con modificazioni dalla l. 17 aprile 2015, n. 43); un'attività che, potendo condurre nei casi più gravi alla rimozione del contenuto dei siti o addirittura al sequestro dei medesimi, potrebbe ripercuotersi sulla libertà di espressione, sulla libertà di iniziativa economica e sul diritto all'onore e alla reputazione. V. al riguardo D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *www.archiviopenale.it*, 2016, n. 1, 5 s., e S. SIGNORATO, *Le misure di contrasto in rete al terrorismo:* black list*, inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio* internet, in R.E. KOSTORIS, F. VIGANÒ (a cura di), *Il nuovo "pacchetto" antiterrorismo*, Torino, 2015, 59 s.

di svolgimento nel decreto di autorizzazione (art. 267 comma 3 c.p.p.), indispensabile per perimetrare un'attività che diversamente, grazie alla estrema duttilità ed invasività dei captatori, comporterebbe un'incursione incontrollata nella *privacy*[17].

Soddisfatte tali condizioni, opera un ulteriore presupposto di validità processuale, ortodossamente ricostruito dalle Sezioni unite della cassazione nella sentenza Scurato del 2016[18]: queste intercettazioni, pienamente legittime nella misura in cui venissero svolte in luoghi pubblici, sarebbero di regola inutilizzabili qualora avvenissero in uno dei luoghi indicati dall'art. 614 c.p. (ossia il domicilio o altro luogo di privata dimora).

Tale divieto, invocabile al momento dello stralcio previsto dall'art. 268 commi 6 s. c.p.p.[19] o, in sede cautelare, ai fini del giudizio di riesame, a seguito della trasmissione alla difesa dei materiali intercettati usati per disporre la misura[20], si ricava dal parametro fissato dall'art. 266 comma 2 c.p.p.: la presenza di un «fondato motivo» di ritenere che in un determinato luogo privato «si sta svolgendo l'attività criminosa». Quest'ultimo, per quanto non debba essere inteso in modo troppo rigoroso[21], in ogni caso presuppone l'indicazione dei luoghi delle captazioni. Con la conseguenza che l'impiego dei *trojan*, per defini-

[17] Cfr. A. GAITO, S. FÙRFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *www.archiviope nale.it*, 2016, n. 2, 16 s.

[18] Cass., Sez. un., 28 aprile 2016, n. 26889.

[19] Durante il quale il giudice, anche su sollecitazione della difesa, dovrebbe dichiarare inammissibili i dati captati nei luoghi privati in rapporto ai quali l'intercettazione non fosse stata autorizzata. Sulle distorsioni pratiche di tale istituto v., peraltro, E.M. CATALANO, *Prassi devianti e prassi virtuose in materia di intercettazioni*, in *Proc. pen. giust*., 2016, n. 1, 5 s.

[20] Tale facoltà è offerta dall'art. 268 c.p.p., dopo la declaratoria di illegittimità ad opera di Corte cost. 10 ottobre 2008, n. 336.

[21] Esso si limita a richiedere la mera possibilità di supporre che, al momento dell'emissione del decreto di autorizzazione, in quel luogo sia in corso un'attività penalmente rilevante. L'intercettazione non sarebbe inammissibile per il solo fatto che, una volta disposta, emergesse che in realtà non si stava compiendo nessun reato. Cfr. A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, 185 s.

zione irriducibili a qualsiasi delimitazione spaziale, porterebbe ad eludere quanto richiesto dal codice[22].

Il problema è che, in applicazione della logica del doppio binario, vige da tempo una deroga al criterio fissato dall'art. 266 comma 2 c.p.p. Si allude alla previsione dell'art. 13 comma 1 d.l. 13 maggio 1991, n. 152[23]; la quale, nei procedimenti per i delitti di «criminalità organizzata», consente le intercettazioni ambientali nei luoghi privati indipendentemente dal contemporaneo svolgimento di un'attività criminosa.

Di qui la facoltà di autorizzare le intercettazioni in questione senza nessuna limitazione spaziale? Una parte della giurisprudenza ha risposto negativamente al quesito, sulla base di un ragionamento che, sebbene non invocandola esplicitamente, ripropone la teoria delle prove incostituzionali. L'unica opzione interpretativa compatibile con il dettato degli artt. 14 e 15 Cost. – si legge in una sentenza della sesta Sezione della Corte di Cassazione – sarebbe «quella secondo la quale l'intercettazione ambientale deve avvenire in luoghi ben circoscritti e individuati *ab origine* e non in qualunque luogo si trovi il soggetto». Le captazioni effettuate in luoghi privati diversi da quelli individuati dall'autorizzazione dovrebbero essere «espunte dall'orizzonte cognitivo e valutativo» del giudice[24].

---

[22] Non varrebbe eccepire che il decreto di autorizzazione potrebbe comunque contenere una delimitazione spaziale (ad esempio indicando solo i luoghi privati abitualmente frequentati dalla persona intercettata), in modo che, laddove tecnicamente possibile, le intercettazioni si sospendano automaticamente ogni volta in cui il dispositivo intercettato venga a trovarsi in un altro luogo privato (v. A. CISTERNA, *Spazio ed intercettazioni, una* liaison *tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite*, in *www.archiviopenale.it*, 2016, n. 2, 1 s.). Come Cass., Sez. un., 28 aprile 2016, cit. ha posto in rilievo, si tratterebbe di un'indicazione meramente formale, concretizzandosi in un'autorizzazione "al buio": il giudice non sarebbe in grado di prevedere dove il dispositivo potrebbe essere collocato, con la "conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari di tipo tradizionale".

[23] Convertito con modificazioni dalla l. 12 luglio 1991, n. 203.

[24] Cfr. Cass., sez. VI, 26 maggio 2015, n. 27100. In dottrina v. L. FILIPPI, *L'ispeperqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)*, in *www.archiviopenale.it*, 2016, n. 2, 2 s.; ID., *Il captatore informatico: l'intercettazione* ubicumque *al vaglio delle Sezioni unite*, in *www.archiviopenale.it*, 2016, n. 1, 2 s.; E. LORENZETTO, *Il peri-*

È consentito replicare che, nei procedimenti di cui si discute, un divieto probatorio non solo non è espressamente previsto dal legislatore, ma è addirittura escluso dalla chiara deroga all'art. 266 comma 2 c.p.p. introdotta dall'art. 13 comma 1 d.l. n. 152 del 1991. Indurlo sulla base della Costituzione porterebbe l'interprete a confondere l'essere con il dover essere, sostituendo le scelte legislative con le proprie preferenze di valore quanto alla sorte delle intercettazioni effettuate nei luoghi privati[25].

Né va trascurato che il requisito della delimitazione spaziale delle intercettazioni non è considerato indefettibile neppure dalla Corte europea dei diritti dell'uomo. I provvedimenti che autorizzano le intercettazioni, stando al *case-law* di Strasburgo, devono chiaramente identificare una specifica persona *o* un singolo insieme di luoghi da sottoporre a sorveglianza[26]. Vale a dire che, nell'ottica della Corte europea, la previsione di una delimitazione spaziale servirebbe ad apprestare una protezione più intensa della *privacy*. Non sarebbe vietato al legislatore rinunciarvi in caso di emergenza, come nei momenti di recrudescenza della minaccia terroristica. L'essenziale è che le intercettazioni, in questi casi, siano ristrette alle sole conversazioni che coinvolgano la persona individuata nel decreto di autorizzazione[27].

Si comprende così perché la sentenza Scurato delle Sezioni unite abbia ritenuto utilizzabili nei procedimenti relativi ai reati individuati dall'art. 13 comma 1 d.l. 152 del 1991 le intercettazioni mediante cap-

*metro delle intercettazioni ambientali eseguite mediante "captatore informatico"*, in *www.penalecontemporaneo.it*, 24 marzo 2016.

[25] Per la critica alla teoria delle prove incostituzionali v. già F. CORDERO, *Tre studi sulle prove penali*, Milano, 1963, 153 s.; ora cfr. F. CAPRIOLI, *Colloqui riservati e prova penale*, Milano, 2000, 236 s. e N. GALANTINI, *Inutilizzabilità della prova e diritto vivente*, in *Riv. it. dir. e proc. pen*., 2012, 76 s.

[26] Così Corte eur. dir. uomo, Grande Camera, 4 dicembre 2015, *Roman Zakharov*, cit., § 264.

[27] Cfr. A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen*., 2016, 2286.

tatore informatico, anche se effettuate in luoghi privati non specificamente individuati dal decreto di autorizzazione[28].

È una lettura difficile da contestare, in quanto ha dalla sua un dato normativo univoco[29]. Da criticare, semmai, è proprio quest'ultimo, nella misura in cui la deroga al requisito della limitazione spaziale delle intercettazioni ambientali – testualmente riferita, come si è detto, ai delitti di «criminalità organizzata» – appare fornita di un ambito applicativo troppo ampio. Tanto è vero che le Sezioni unite hanno identificato i delitti in questione non solo con quelli elencati nell'art. 51, commi 3 *bis* e 3 *quater* c.p.p., ma anche con tutti i delitti «comunque facenti capo a un'associazione per delinquere», «con esclusione del mero concorso di persone nel reato»[30].

Il principio di proporzionalità che dovrebbe regolamentare la compressione del diritto alla riservatezza, per converso, suggerirebbe di circoscriverli maggiormente; in particolare limitandoli ai soli reati associativi che, sulla base delle caratteristiche e della potenziale pericolosità del programma criminoso perseguito, sono puniti dal legislatore con le pene più elevate[31]. Un esito conseguibile solo attraverso una mo-

[28] Cfr. Cass., Sez. un., 28 aprile 2016, cit. Analogamente sez. VI, 10 marzo 2016, n. 13884, che aveva rimesso la questione alle Sezioni unite, nonché Id., 8 aprile 2015, n. 27536, e 12 marzo 2015, n. 24237.

[29] Si veda A. BALSAMO, *Le intercettazioni*, cit., 2284 s. Cfr. pure M. CAIANIELLO, *Osservazioni sul documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*.

[30] Cass., Sez. un., 28 aprile 2016, cit. Criticano tale lettura estensiva G. SPANGHER, *La riforma Orlando della giustizia penale: prime riflessioni*, in *www.penalecontemporaneo.it*, 5 ottobre 2016, 16 s., e P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. giust.*, 2016, n. 5, 136 s.

[31] In questo senso v. la memoria della Procura generale presso la Corte di Cassazione, redatta da A. BALSAMO e A. ROSSI, 20, in *http://www.questionegiustizia.it/doc/memoria-ssuu-procura-generale-trojan.pdf*, secondo cui la categoria in questione potrebbe essere ricavata da «una rigorosa ricognizione di carattere sistematico del concetto di criminalità organizzata desumibile dall'ampio complesso di dati normativi esistenti nel nostro ordinamento, e dunque certamente comprensiva delle associazioni con finalità di terrorismo e di eversione dell'ordine democratico (art. 270 *bis* c.p.), delle associazioni di tipo mafioso (art. 416 *bis* c.p.) e delle associazioni finalizzate al traffico illecito di stupefacenti di cui all'art. 74 del d.P.R. n. 309 del 1990». Cfr. pure A. TESTAGUZZA,

difica legislativa o, perlomeno, una declaratoria di incostituzionalità per violazione del diritto alla riservatezza informatica, considerato che non potrebbero essere gli interpreti a fissare caso per caso le soglie edittali rilevanti a questo proposito[32].

Fortunatamente, per quanto riguarda i delitti «con finalità di terrorismo», una delimitazione più netta è già stata operata dall'art. 3 comma 1 d.l. 18 ottobre 2001 n. 374[33]: le intercettazioni ambientali in deroga al requisito dell'art. 266 comma 2 c.p.p. sono consentite solo in rapporto ai delitti previsti dall'art. 407 comma 2 lett. *a* n. 4 c.p.p., ossia quelli puniti con la reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni[34], nonché ai delitti *ex* artt. 270 *ter* e 280 *bis* c.p.[35]. Una previsione destinata a prevalere in virtù del canone *lex specialis derogat generali*.

Alle intercettazioni tradizionali si affiancano quelle preventive *ex* art. 226 disp. att. c.p.p., autorizzabili dal pubblico ministero su richiesta del Ministro dell'interno, dei servizi di *intelligence*, del questore, del comandante provinciale dei carabinieri o della guardia di finanza. Queste ultime possono essere effettuate – magari tramite *trojan* – anche «se avvengono nei luoghi indicati dall'art. 614 c.p.»; il che significa che, non essendo stato neppure in questo caso riprodotto il requisito fissato

---

Exitus acta probat *"Trojan" di Stato: la composizione di un conflitto*, in *www.archivio penale.it*., 2016, n. 2, 7 s.

[32] Cfr. G. LASAGNI, *L'uso di captatori informatici (*trojans*) nelle intercettazioni "fra presenti"*, in *www.penalecontemporaneo.it*, 7 ottobre 2016, 18 s.

[33] Convertito con modificazioni dalla l. 15 dicembre 2001 n. 438, e poi modificato dalla l. 14 febbraio 2003, n. 34.

[34] Vale a dire il delitto di associazione con finalità di terrorismo (art. 270 *bis* c.p.), ma anche, tra gli altri, i delitti di arruolamento (art. 270 *quater* c.p.) e di addestramento o auto-addestramento (art. 270 *quinquies* c.p.). Sull'auto-addestramento, fattispecie introdotta dal d.l. n. 7 del 2015 a seguito dell'attentato terroristico presso la sede del giornale *Charlie Hebdo* a Parigi, con l'intento di anticipare la soglia di punibilità dei c.d. «lupi solitari», v. A. VALSECCHI, *Le modifiche alle norme incriminatrici in materia di terrorismo*, in R.E. KOSTORIS, F. VIGANÒ (a cura di), *Il nuovo "pacchetto"*, cit., 10 s., e R. WENIN, *L'addestramento per finalità di terrorismo alla luce delle novità introdotte dal d.l. 7/2015*, in *www.penalecontemporaneo.it*, 3 aprile 2015.

[35] Ossia il delitto di assistenza agli associati, punito con la reclusione fino a quattro anni, e il delitto di atti di terrorismo con ordigni micidiali o esplosivi, punito con la reclusione da due e cinque anni.

dall'art. 266 comma 2 c.p.p., anche esse non subiscono nessuna delimitazione spaziale.

Il d.l. n. 7 del 2015 le ha estese a qualsiasi delitto con finalità di terrorismo commesso «mediante l'impiego di tecnologie informatiche o telematiche», aumentando altresì a ventiquattro mesi il termine massimo di conservazione dei dati captati. Ma questo loro più ampio raggio operativo appare compensato dalla circostanza che, stando al comma 5 dell'art. 226 disp. att., «gli elementi acquisiti attraverso le attività preventive non possono essere utilizzati nel procedimento penale, fatti salvi i fini investigativi»; «le attività di intercettazione» e le «notizie acquisite a seguito delle attività medesime», inoltre, «non possono essere menzionate in atti di indagine né costituire oggetto di deposizione né essere altrimenti divulgate».

È, così, inibito l'impiego dei dati captati per disporre una misura cautelare o un mezzo di ricerca della prova, quale un'ispezione, una perquisizione o un'intercettazione *ex* art. 266 c.p.p.[36]. Ne viene, nondimeno, autorizzato l'uso "investigativo". Vale a dire che al più potrebbero giustificare ulteriori attività di tipo proattivo, prodromiche alla successiva instaurazione di un procedimento a carico dei sospetti terroristi: assunzione di informazioni da persone estranee alle attività criminose o da collaboratori di giustizia, osservazioni, controlli, pedinamenti, rilievi ed accertamenti tecnici ripetibili, indagini sotto copertura[37].

[36] Cfr. F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, in G. DI CHIARA (a cura di), *Il processo penale tra politiche della sicurezza e nuovi garantismi*, Torino, 2003, 22 s.; G. GARUTI, *Le intercettazioni preventive nella lotta al terrorismo internazionale*, in *Dir. pen. proc*., 2005, 1460 s.; T. RAFARACI, *Intercettazioni e acquisizione di tabulati telefonici*, in R.E. KOSTORIS, R. ORLANDI (a cura di), *Contrasto al terrorismo interno e internazionale*, Torino, 2006, 270 s.; A. VELE, *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Padova, 2011, 45 s.

[37] Le quali, ai sensi dell'art. 9 l. 16 marzo 2006, n. 146, potrebbero essere svolte dagli ufficiali di polizia giudiziaria, con il controllo del pubblico ministero, al fine di acquisire elementi di prova, tra l'altro, «in ordine ai delitti commessi con finalità di terrorismo». Sulle indagini volte al reperimento delle *notitiae criminis* v., più in generale, A. ZAPPULLA, *La formazione della notizia di reato. Condizioni, poteri ed effetti*, Torino, 2012, 264 s.

### *4.2. Le videoriprese come* panopticon

I *trojan* sono utilizzabili anche per attivare e controllare a distanza le videocamere dei dispositivi informatici, consentendo di svolgere videoriprese pure all'interno di luoghi privati. È noto come in questo caso venga in gioco una materia non disciplinata dal legislatore, che ha trovato una declinazione normativa in una decisione delle Sezioni unite della cassazione[38].

Le Sezioni unite hanno ricondotto le videoriprese appositamente disposte dagli organi inquirenti ai fini di un procedimento, e non riguardanti comportanti comunicativi[39], alla categoria delle prove atipiche[40], ritenendole utilizzabili, se effettuate in luoghi pubblici, a seguito del vaglio nel contraddittorio con le parti in merito alle «modalità di assunzione» previsto dall'art. 189 c.p.p.

Non così, invece, riguardo alle videoriprese in luoghi privati: non potrebbe considerarsi acquisibile nelle forme dell'art. 189 c.p.p. – ha rilevato la Corte – «la prova basata su un'attività che la legge vieta, come nel caso delle riprese visive di comportamenti non comunicativi avvenuti in ambito domiciliare»[41]. Ma si tratta di un'inutilizzabilità co-

[38] Si allude a Cass., Sez. Un., 28 marzo 2006, n. 26795, la cui impostazione è stata ripresa dalla già citata decisione della sez. VI, 26 maggio 2015, n. 27100, riguardo alle videoriprese effettuate tramite *trojan*.

[39] Diversamente dovrebbe applicarsi la disciplina delle intercettazioni *ex* artt. 266 s. c.p.p.

[40] Quest'ultima, come rilevano sempre le Sezioni unite, non va confinata alle sole prove formate in dibattimento, ma è estendibile alle prove raccolte durante le indagini. Nulla vieta, infatti, di intendere il contraddittorio «sulle modalità di assunzione» richiesto dall'art. 189 c.p.p. come posticipato anziché anticipato: cfr. A. CAMON, *Le Sezioni Unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni nuovi dubbi*, in *Riv. it. dir. proc. pen*., 2006, 1556 s. *Contra* v. O. MAZZA, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont*., *riv. trim*., 2013, n. 3, 9.

[41] In senso adesivo, con diverse sfumature, v. A. CAMON, *Le Sezioni Unite*, cit., 1561 s.; O. MAZZA, *I diritti fondamentali*, cit., 9 s.; M.L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni Unite*, in *Cass. pen*., 2006, 3958 s.; F. MORELLI, *Videoriprese mediante la* webcam *di un* computer *illecitamente sottratto e tutela del domicilio*, in *Dir. pen. proc*., 2013, 477; F. RUGGIERI, *Riprese visive e inammissibilità*

struita sulla base di un ragionamento che, per quanto la Corte abbia tentato di negarlo, risulta anche esso fondato sulla teoria delle prove incostituzionali[42], risolvendosi dunque in un *wishful thinking*. Le scarne previsioni dell'art. 189 c.p.p. altro non permettono che sollevare una questione di legittimità costituzionale per violazione del requisito di precisione imposto dalla riserva di legge *ex* art. 14 Cost.[43].

Le Sezioni unite hanno aggiunto che le videoriprese in luoghi meramente riservati[44] – i quali, a differenza dei luoghi privati, non fruiscono della tutela apprestata dall'art. 14 Cost. – sarebbero dal canto loro utilizzabili solo qualora venissero disposte con un provvedimento motivato dell'autorità giudiziaria. Si tratta, però, di un assetto normativo arbitrariamente costruito dall'interprete, e comunque incompleto[45]. Perché, in particolare, l'autorizzazione dell'autorità giudiziaria, e non di un vero e proprio giudice, come invece previsto dall'art. 266 c.p.p. in rapporto alle intercettazioni (ossia un mezzo investigativo altrettanto intrusivo per la *privacy*)? Quali, inoltre, i requisiti di ammissibilità su cui dovrebbe cadere la motivazione?

Di per sé, la disciplina minimale delle prove atipiche non appare in grado di fornire un adeguato compendio di garanzie alle videoriprese

---

*della prova*, in *Cass. pen*., 2006, 3948 s.; P. TONINI, C. CONTI, *Il diritto delle prove penali*, II ed., Milano, 2014, 105 s., 201 s.

[42] V. A. CAMON, *Le Sezioni Unite*, cit., 1560 s.

[43] Cfr. F. CORDERO, *Procedura penale*, IX ed., Milano, 2012, 851. V. pure F. CAPRIOLI, *Nuovamente al vaglio della Corte costituzionale l'uso investigativo degli strumenti di ripresa visiva*, in *Giur. cost.*, 2008, 1836 s.; M. DANIELE, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen*., 2013, 369 s.; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007, 149 s.; con specifico riguardo alle attività di localizzazione satellitare tramite *tracker GPS*, S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, 607.

[44] Ad esempio, i bagni dei locali pubblici, o i *privé* delle discoteche.

[45] Si vedano, anche per ulteriori critiche, E. ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra* standard *di tutela della* privacy *e onde eversive*, in *www.archiviopenale.it*, 2015, n. 3, 14 s.; S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2015, 774 s.; A. SCALFATI, O. BRUNO, *Orientamenti in tema di videoriprese*, in *Proc. pen. giust*., 2011, n. 1, 101; N. TRIGGIANI, *Le videoriprese investigative*, in A. SCALFATI (a cura di), *Le indagini atipiche*, 158 s.

nei luoghi privati o, comunque, riservati. Ma tale conclusione è suscettibile di mutare qualora si consideri l'art. 189 c.p.p. non solo in un'ottica puramente interna, ma anche con la lente dell'interpretazione conforme alla CEDU e alle sentenze della Corte europea dei diritti dell'uomo. Queste ultime, pur calibrate sulle specificità di ciascun caso concreto, non omettono di indicare taluni principi e criteri orientativi da cui è possibile enucleare le garanzie processuali indefettibili in merito alla compressione dei vari diritti. Si tratta di *guideline* che integrano parametri normativi di rango superiore rispetto alla legge ordinaria[46], ed appaiono pertanto capaci di arricchire il testo dell'art. 189 c.p.p., precisando le «modalità di assunzione» delle prove atipiche.

Di qui un ulteriore passaggio ermeneutico: dovendo "innestare" nell'art. 189 c.p.p. le prescrizioni processuali suggerite dalla Corte europea, il giudice potrebbe applicare in via estensiva la disciplina già prevista dal legislatore italiano in rapporto ad analoghi mezzi investigativi tipici, nella misura in cui ponesse garanzie corrispondenti a quelle richieste dal *case-law* di Strasburgo.

Questo parrebbe essere proprio il caso delle videoriprese effettuate dagli organi inquirenti in modo tale da interferire con il diritto alla *privacy*. Come si è già detto[47], la Corte europea esige che le attività di captazione occulta di dati riservati nei procedimenti penali siano regolate da norme di legge conoscibili e prevedibili, nonché in grado di conseguire un bilanciamento proporzionato fra i valori in gioco, mediante la previsione di adeguate ed effettive garanzie volte ad evitare abusi di potere[48]. Ma garanzie del genere sono rinvenibili nelle norme sulle in-

[46] Per quanto soggetti al margine di apprezzamento interno: v. M. DANIELE, *Norme processuali convenzionali e margine di apprezzamento nazionale*, in *Cass. pen*., 2015, 1694 s.

[47] Cfr. *supra*, § 2.

[48] Cfr. Corte eur. dir. uomo, Grande Camera, 4 dicembre 2015, *Roman Zakharov*, cit., § 227 s., la quale in particolare richiede: l'indicazione sufficientemente chiara e precisa dei presupposti fattuali della captazione, nonché delle categorie dei reati e delle persone in rapporto a cui la medesima può essere svolta; l'autorizzazione o il controllo successivo da parte di un organo indipendente dal potere esecutivo; l'indicazione dei limiti di durata della captazione; la procedura da osservare per l'uso in giudizio, la comunicazione agli interessati, la conservazione e la distruzione dei dati captati. Quanto

tercettazioni di comunicazioni; le quali, considerata la somiglianza fra le intercettazioni e le videoriprese, potrebbero essere integralmente applicate anche a queste ultime, nella ragionevole convinzione che si tratti di una disciplina in linea con la volontà del legislatore e compatibile con la CEDU[49].

Accogliendo tale impostazione, le videoriprese effettuate dagli organi inquirenti, tanto con modalità tradizionali quanto tramite *trojan*, andrebbero sottoposte al regime delle intercettazioni sonore *ex* art. 266 s. c.p.p. e 226 disp. att. quanto ai presupposti di ammissibilità, alle modalità di svolgimento e all'utilizzabilità processuale[50]. Esse verrebbero così sottratte alle deformalizzazioni operate dalla giurisprudenza, per essere disciplinate da regole in linea con le indicazioni del *case-law* della Corte europea. Ne deriverebbe inoltre una disciplina uniforme, superando l'inconveniente – generato dalla lettura delle Sezioni unite – di dover osservare requisiti giuridici differenti a seconda dell'oggetto della captazione (immagini oppure mere comunicazioni sonore); il che spesso determina problemi insuperabili nella pratica, a causa dell'impossibilità di prevedere *ex ante* l'esito dell'intrusione[51].

alle intercettazioni preventive, v. Id., sez. IV, 18 maggio 2010, *Kennedy c. Regno Unito*, § 118 s.

[49] *Contra* O. MAZZA, *I diritti fondamentali*, cit., 9 s., secondo cui, rappresentando le videoriprese un mezzo investigativo vietato, l'operazione si tradurrebbe in un'estensione analogica *in malam partem* della disciplina delle intercettazioni.

[50] La Corte europea, peraltro, non richiede necessariamente l'inutilizzabilità dei risultati delle captazioni effettuate in violazione delle regole in questione, ma si accontenta di una valutazione del loro impatto sull'equità del procedimento considerata nel suo complesso: v. ad esempio Corte eur., Grande Camera, *Bykov c. Russia*, 10 marzo 2009, § 84 s., nonché M. DANIELE, *Indagini informatiche*, cit., 370 s. Ma eventuali regole di esclusione specificamente previste a livello nazionale – o comunque, come nel nostro caso, ricavate dall'interpretazione estensiva – sarebbero ovviamente compatibili con la giurisprudenza di Strasburgo.

[51] V. al riguardo F. MORELLI, *Videoriprese*, cit., 478 s.

### *4.3. Le perquisizioni* on-line *e un'auspicabile ibridazione degli strumenti repressivi e preventivi*

Resta da considerare un'ultima categoria di indagini occulte: le c.d. perquisizioni *on-line*, le quali si concretizzano nell'uso dei *trojan* per captare i contenuti dei dispositivi informatici (dati rinvenibili nell'*hard disk*, informazioni visualizzate sullo schermo, *password* digitate tramite la tastiera), nonché per il monitoraggio delle attività in rete compiute attraverso i medesimi. Sono indagini ancora più insidiose per la *privacy*, per l'evidente ragione che, a differenza delle intercettazioni e delle videoriprese, non si limitano ai suoni e alle scene che avvengono in prossimità dei dispositivi, ma sondano questi ultimi nella loro completezza: spazi teoricamente inviolabili che rappresentano le estensioni digitali della personalità degli individui, dove vengono riversate informazioni riservate di ogni genere. Sono, al contempo, indagini ancora più efficaci soprattutto nell'ottica della prevenzione, poiché consentono una sorveglianza costante delle attività dei sospetti terroristi.

Ciò spiega come si tratti di un mezzo investigativo piuttosto discusso. Esso può farsi rientrare nel paradigma delle intercettazioni *ex* art. 266 *bis* c.p.p. nella misura in cui si concretizzi in una captazione delle comunicazioni e dei messaggi in entrata e in uscita (conversazioni tramite *skype* o programmi analoghi, *chat*, *e-mail*, *sms*, *mms*)[52]. Al di là di queste ipotesi, le perquisizioni *on-line* al momento non sono disciplinate nel nostro sistema[53]. Figuravano in una prima versione del d.l. n. 7 del 2015, poi abbandonata dal Governo, con una formulazione che ora è

[52] Cfr. E.M. MANCUSO, *L'acquisizione di contenuti* e-mail, in A. SCALFATI (a cura di), *Le indagini*, cit., 78 s.

[53] Nel senso, invece, che sarebbero applicabili alle perquisizioni *on-line* le norme in tema di perquisizioni dei sistemi informatici *ex* art. 247 comma 1 *bis* c.p.p., v. A. TESTAGUZZA, Digital forensics, cit., 90 s., e M. TORRE, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. proc*., 2015, 1171 s. Tuttavia, adottando tale impostazione, dovendo consentire la partecipazione del difensore ai sensi degli artt. 356 e 365 c.p.p., le operazioni in questione perderebbero il loro carattere segreto e, dunque, buona parte della loro valenza conoscitiva. Inoltre esse sarebbero sottoposte all'autorizzazione del solo pubblico ministero anziché di un giudice, e senza alcuna limitazione quanto alla tipologia di reato oggetto del procedimento.

stata ripresa dal d.d.l. C-3470[54]. Vi si prevede la loro qualificazione quali intercettazioni «del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi» *ex* art. 266 *bis* c.p.p., svolte «attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico».

Per quanto l'adozione delle garanzie previste dagli artt. 266 s. c.p.p. sarebbe apprezzabile, risulterebbe però irragionevole permettere le perquisizioni *on-line* in relazione agli stessi reati in merito ai quali sono consentite le intercettazioni telematiche: ovvero i reati elencati dall'art. 266 c.p.p., nonché «i reati commessi mediante l'impiego di tecnologie informatiche o telematiche». È un insieme eterogeneo di illeciti di diversa natura e gravità, in rapporto a molti dei quali le perquisizioni *on-line* risulterebbero uno strumento sproporzionato. Per quanto concerne, in particolare, i reati di terrorismo, esse andrebbero limitate alle fattispecie più gravi: perlomeno quelle punite con la reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, per le quali come abbiamo visto sono consentite le intercettazioni tramite *trojan* senza limitazioni spaziali.

Si deve aggiungere che la pervasività dei mezzi investigativi in questione ne suggerirebbe un'ulteriore restrizione del campo operativo. I loro esiti, più precisamente, non dovrebbero possedere valore probatorio – né in giudizio né ai fini dell'applicabilità di una misura cautelare – ma unicamente investigativo. Vale a dire che sarebbe auspicabile configurare le perquisizioni *on-line* come uno strumento di tipo ibrido: autorizzabili di regola da un giudice in base a condizioni analoghe a quelle previste dagli artt. 266 s. c.p.p., dovrebbero però possedere la medesima sfera di utilizzo delle intercettazioni preventive *ex* art. 226 disp. att. c.p.p., nonché avere precisi limiti temporali di durata[55].

[54] Presentato il 2 dicembre 2015.

[55] Spunti al riguardo sono suscettibili di provenire, più in generale, dalla giurisprudenza costituzionale tedesca del *Bundesverfassungsgericht*. Si pensi alla sentenza del 27 febbraio 2008, che ha dichiarato illegittima la normativa nazionale in materia per contrasto con il diritto alla riservatezza dei sistemi informatici, inteso come espressione del più generale diritto alla dignità, su cui cfr. R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* Online Durchsuchung in *Riv. trim. dir. pen. ec.*,

## *5. I pericoli dell'inerzia legislativa*

Se sarebbe inopportuno introdurre una disciplina come quella rinvenibile nel d.d.l. C-3470, appare persino più grave l'errore simmetrico: la perseveranza del legislatore nel rinunciare a disciplinare le perquisizioni *on-line*[56]. È un atteggiamento dettato da calcoli di tipo utilitaristico: si evita di introdurre uno strumento investigativo così pericoloso per la *privacy* per non perdere il consenso dell'opinione pubblica. Ma esso porta anche ad ignorare una realtà che, per quanto sgradevole, non può essere dimenticata: mezzi del genere, sempre più accessibili grazie all'evoluzione della tecnologia, vengono comunque utilizzati nella prassi, specie per contrastare le forme di criminalità che generano il massimo allarme sociale. E in assenza di una regolamentazione precisa, inevitabilmente aumenta il rischio che siano utilizzati in modo arbitrario[57].

Non fruendo al momento di un'apposita disciplina, eventuali perquisizioni *on-line* che venissero disposte dagli organi inquirenti, a rigore, dovrebbero essere ritenute addirittura giuridicamente inesistenti[58]. Ciò

---

2009, 695 s. Si veda anche la più recente sentenza del 20 aprile 2016, su cui cfr. L. GIORDANO, A. VENEGONI, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *www.penalecontemporaneo.it*, 8 maggio 2016.

[56] Sottolineano la necessità e l'urgenza di un intervento del legislatore M.T. ABBAGNALE, *In tema di captatore informatico*, in *www.archiviopenale.it*, 2016, n. 2, 7 s., e L. PICOTTI, *Spunti di riflessione*, cit., 9 s. Si veda anche *Necessaria una disciplina legislativa in materia di captatori informatici (c.d. 'trojan'): un appello al legislatore da parte di numerosi docenti di diritto italiani*, in *www.penalecontemporaneo.it*, 7 ottobre 2016.

[57] Si veda A. SCALFATI, *Un ciclo giudiziario "travolgente"*, in *Proc. pen. giust.*, 2016, n. 4, 115.

[58] Ritengono invece configurabile un'inutilizzabilità per contrasto con le norme della Costituzione e della Convenzione europea, C. CONTI, M. TORRE, *Spionaggio informatico nell'ambito dei* social network, in A. SCALFATI (a cura di), *Le indagini*, cit., 429; F. IOVENE, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont.*, *riv. trim.*, 2014, n. 3-4, 341; S. MARCOLINI, *Le cosiddette perquisizioni on-line (o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, 2864 s. V. anche S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *www.archiviopenale.it*, 2014, n. 1, 10 s. il quale, rilevando in questo caso la

perché esse, consistendo in captazioni occulte ed indiscriminate di tutti i dati contenuti negli spazi virtuali riservati delle persone, non possiederebbero i requisiti minimi indispensabili per integrare lo schema normativo dei mezzi investigativi[59]. Questi ultimi consistono in attività di ricerca di prove fisiche o digitali compiute da esseri umani (si pensi alle ispezioni e alle perquisizioni); oppure in attività che, pur se svolte mediante invisibili dispositivi elettronici, hanno un oggetto limitato (come avviene per le intercettazioni e le videoriprese, che riguardano singoli suoni od immagini). Né, per la medesima ragione, le perquisizioni *on-line* potrebbero entrare nei procedimenti penali attraverso la breccia dell'art. 189 c.p.p.

Non sempre, però, la giurisprudenza ha mostrato di cogliere a pieno le peculiarità delle perquisizioni *on-line*. Basti pensare ad una sentenza con cui la quinta Sezione della Corte di Cassazione ha ritenuto ammissibili come prove documentali *ex* art. 234 c.p.p. i *file* carpiti tramite un *trojan* da un *personal computer*. La Corte, in quel caso, non ha considerato violato il diritto alla riservatezza per la ragione che il *computer* era situato in un ufficio aperto al pubblico, ed erano stati acquisiti unicamente alcuni documenti predisposti per essere stampati su supporto cartaceo ed essere poi consegnati al loro destinatario[60]. Agevole replicare come l'attività investigativa fosse in realtà avvenuta all'interno di uno spazio, per quanto virtuale, altamente sensibile, senza fruire delle dovute garanzie processuali.

---

commissione del delitto di accesso abusivo ad un sistema informatico (art. 615 *ter* c.p.), invoca la categoria delle prove illecite.

Più in generale, S. MARCOLINI, *Le indagini atipiche*, cit., 787 s., costruisce l'inutilizzabilità dei mezzi di investigazione atipici lesivi della riservatezza sulla base della decisione della Corte di giustizia dell'Unione europea dell'8 aprile 2014, *Digital Rights Ireland Ltd*, C-293/12 e C-594/12, § 26 s., che ha ritenuto invalida la Direttiva 2006/24/CE del 15 marzo 2006 sulla conservazione dei dati di traffico per violazione del diritto alla *privacy*. Ma si può obiettare che la sentenza in questione disciplina solo la *retention* dei dati di traffico, e inoltre non si occupa specificamente della sorte processuale dei dati conservati in base alle norme giudicate invalide.

[59] *Mutatis mutandis*, analogo il ragionamento di F. CORDERO, *Procedura penale*, VI ed., Milano, 1982, 852 s., per giustificare l'inesistenza delle confessioni e delle testimonianze estorte, non sottoposte ad esplicite regole di esclusione dal c.p.p. 1930.

[60] V. Cass., Sez. V, 14 ottobre 2009, n. 16556.

In una diversa occasione la quarta Sezione della Corte ha, invece, annullato una perquisizione e il conseguente sequestro concernenti il sistema informatico di prenotazione dei voli *on-line* della *Ryanair*[61], opportunamente rilevando come si fosse trattato di un «preventivo ed indefinito monitoraggio» del medesimo «in attesa dell'eventuale e futura comparsa del dato da acquisire»[62]; ossia un «nuovo ed anomalo strumento di ricerca della prova, con finalità nettamente esplorative, di mera investigazione», «che nulla ha a che fare con la perquisizione»[63].

Queste oscillazioni, perniciose per la certezza del diritto e per la parità di trattamento, si spiegano proprio con l'assenza di una disciplina. Altro non sono che l'inevitabile conseguenza della mancanza di coraggio del legislatore, il quale continua a lasciare la concreta regolamentazione di un mezzo investigativo così importante ma, al contempo, così insidioso alle preferenze assiologiche della giurisprudenza.

[61] Cfr. Cass., Sez. IV, 17 aprile 2012, n. 19618.

[62] Motivato dall'esigenza di identificare in tempo utile, in base a parametri sintomatici desumibili dalle modalità di prenotazione dei voli (si pensi alle prenotazioni eseguite *last minute*, in orario notturno, con rientro programmato entro pochissimo tempo dall'arrivo), i passeggeri che avrebbero potuto trasportare sostanze stupefacenti.

[63] Cfr. G. BONO, *Il divieto di indagini* "ad explorandum" *include i mezzi informatici di ricerca della prova*, in *Cass. pen*., 2013, 1525 s.

# CONTRASTO AL TERRORISMO, INDAGINI INFORMATICHE E TUTELA DEI DIRITTI FONDAMENTALI

*Federica Iovene*

SOMMARIO: *1. Introduzione. 2. Caratteristiche delle indagini informatiche. 3. Le c.d. perquisizioni* online*. 4.* Data retention*. 5. Conclusioni.*

## *1. Introduzione*

Quando si affronta il tema delle c.d. indagini informatiche non si può che muovere da una duplice constatazione: il rapporto di forte tensione con i diritti fondamentali della persona e le difficoltà di adattamento alle categorie tradizionali.

La storia recente di alcuni strumenti investigativi mostra chiaramente quale sia l'approccio a queste problematiche, ad una prima fase in cui la prassi recepisce e sfrutta il portato dell'evoluzione tecnologica, segue una seconda fase in cui interviene la giurisprudenza nel tentativo di regolamentare l'utilizzo di determinate tecniche investigative nel rispetto dei principi costituzionali e delle norme del codice[1]; talvolta poi – an-

[1] Valga per tutti l'esempio delle video-riprese. I principi che oggi governano la materia sono quelli dettati dalle Sezioni Unite nella nota sentenza Prisco del 2006 e dalla Corte costituzionale nella sentenza n. 135 del 2002.

Cass., Sez. un. 28 marzo 2006, n. 26795, Prisco, con nota di M.L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni Unite*, e di F. RUGGIERI, *Riprese visive e inammissibilità della prova*, in *Cass. pen.*, 2006, 3937 s.; e di A. CAMON, *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento ed alcuni dubbi nuovi*, in *Riv. it. dir. e proc. pen.*, 2006, 1550 ss.

C. cost., sentenza 24 aprile 2002, n. 135, in *Giur. cost.*, 2002, 1062 ss., con osservazioni di F. CAPRIOLI, *Riprese visive nel domicilio e intercettazioni «per immagini»*.

Non si tratta di una peculiarità dell'ordinamento italiano, bensì di una tendenza diffusa anche in altri ordinamenti. Sul punto si rinvia a G. DI PAOLO, *Judicial Investigations and Gathering of Evidence in a Digital, Online Context*, in *Revue Internationale*

che se sarebbe auspicabile che ciò succedesse sempre – si assiste ad una terza fase in cui interviene il legislatore a disciplinare organicamente la specifica attività[2].

Queste problematiche sono acuite nell'ambito del contrasto al terrorismo dalla sottile linea di confine tra attività di prevenzione e di *intelligence* ed attività repressiva dei reati vera e propria.

Scopo del presente contributo non è quello di illustrare tutte le problematiche che si pongono in tema di indagini e prova informatica, bensì quello di dar conto delle tensioni di cui sopra attraverso l'esame di due attività emblematiche in tal senso. Da un lato le c.d. perquisizioni *online*, dall'altro la c.d. *data retention*, ossia la conservazione e acquisizione di dati di traffico telefonico e telematico.

Preliminare ad ogni approfondimento è però la descrizione sintetica delle principali caratteristiche delle indagini informatiche.

## *2. Caratteristiche delle indagini informatiche*

Innanzitutto va evidenziato che il sistema informatico è un sistema complesso, contenente una moltitudine diversificata di dati. Il termine dati informatici, infatti, è riassuntivo di una pluralità di informazioni, di diversa natura, in grado di circolare con grande facilità e rapidità, prive di una dimensione fisica, ma che necessitano di un supporto fisico per poter essere intellegibili, duplicabili su più supporti, pur rimanendo sempre uguali a se stesse.

Prima caratteristica è quindi la promiscuità dei dati e la loro sostanziale uniformità[3].

---

*de Droit Pénal*, 2009, vol. 1-2, 201-246, ove viene fatto riferimento all'approccio seguito in Italia, negli Stati Uniti e in Canada e si ravvisa per l'appunto questo *trend* comune.

[2] Ciò è accaduto nel caso dei tabulati telefonici che il legislatore dopo una fase di incertezza iniziale ha disciplinato attraverso l'introduzione dell'art. 132 *codice privacy* (d.lgs. 196/2003).

[3] È certamente vero che ogni *file* ha una sua estensione (*doc*, *jpeg*, *pdf*, etc.) che dall'esterno lascia intuire quale sia il contenuto del *file* stesso, ma è altresì vero che se ci si ferma al dato informatico inteso come sequenza di *bit*, ogni dato è uguale ad un altro.

Inoltre, da un punto di vista tecnico non è allo stato ancora possibile un accesso selettivo al sistema informatico. Ciò significa da un lato che le indagini sono sempre lesive della riservatezza e della sicurezza dei dati e delle informazioni – punto questo che verrà approfondito nell'esaminare le c.d. perquisizioni *online* – e dall'altro che alto è il rischio che attività di indagine si trasformino in attività esplorative, volte alla ricerca della *notitia criminis*. Questo rischio è tanto più attuale nell'ambito delle attività di contrasto al terrorismo in cui la linea di confine tra prevenzione e repressione, come già anticipato, è molto labile, poiché i reati da perseguire e quelli da prevenire rimandano ad uno stesso fenomeno criminoso e quindi una stessa attività può presentarsi come preventiva rispetto ad un reato e repressiva rispetto ad un altro[4].

Per descrivere questo meccanismo circolare legato soprattutto al contrasto alla criminalità organizzata e terroristica si è efficacemente parlato di indagini proattive – *proactive investigations* – ossia di quelle attività il cui oggetto è

> l'accertamento *[dell'organizzazione]* delle associazioni dedite alla commissione di reati o al terrorismo, e che sono finalizzate a prevenire la preparazione e la commissione di tali reati così come al reperimento di indizi utili per avviare indagini penali contro quelle associazioni e/o i loro membri[5].

Tali indagini, contrapposte a quelle reattive, costituiscono una sorta di *tertium genus* tra attività preventiva condotta dalla polizia di sicurezza e indagini penali in senso stretto poste in essere dalla polizia giudiziaria[6].

---

Per una più ampia disamina delle caratteristiche delle indagini informatiche, si veda G. DI PAOLO, *(voce) Prova informatica (diritto processuale penale)*, in *Enc. dir.*, *Annali VI*, Milano, 2013, 736 ss.; M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, 283 ss.

[4] R.E. KOSTORIS, *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella risoluzione del XVIII Congresso internazionale di diritto penale*, in *Riv. dir. proc.*, 2010, 239.

[5] Definizione contenuta nella Risoluzione del XVIII Congresso internazionale di diritto penale, come riportato da R.E. KOSTORIS, *La lotta al terrorismo*, cit.

[6] Cfr. S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, 760, secondo cui la distinzione tra indagini

L'idea, come suggerisce il termine stesso, è che tali indagini possano al tempo stesso trarre spunto da indagini penali già avviate nei confronti dell'organizzazione criminosa, e stimolare l'attivazione di nuove indagini qualora emergano notizie di reato[7].

Le c.d. perquisizioni *online* si pongono certamente in questo ambito, presentando potenzialità che possono essere sfruttate nell'ambito del meccanismo circolare descritto.

Infine, non si deve dimenticare che lo spazio informatico è ontologicamente globale e refrattario a limitazioni nazionali. I dati informatici, infatti, sono spesso salvati su *servers* o *personal computers* dislocati in Paesi diversi da quello in cui le indagini vengono svolte – si pensi ad esempio ai servizi di *cloud computing* ma anche ai *server* che forniscono servizi di *web mail* –.

Si pongono quindi seri problemi di cooperazione giudiziaria, soprattutto in considerazione del forte rischio che ogni Stato svolga investigazioni informatiche anche oltre i confini della propria sovranità, fino a che la tecnologia lo consenta, dando vita a quello che è stato efficacemente descritto come una sorta di «"far-west tecnologico", in cui il diritto soccombe alla tecnologia»[8].

Non è questa la sede per affrontare questa ampia tematica, ma è un aspetto che non si può trascurare soprattutto nell'analisi degli strumenti di contrasto al terrorismo, fenomeno che assume al giorno d'oggi una dimensione ontologicamente internazionale.

## *3. Le c.d. perquisizioni* online

Il termine perquisizioni *online* deriva dal tedesco *Online Durchsuchung* ed è riassuntivo di una serie di attività volte ad esplorare e moni-

proattive e indagini reattive solo superficialmente sarebbe sovrapponibile a quella tra attività di polizia preventiva o di sicurezza e attività di polizia giudiziaria.

[7] Cfr. R.E. KOSTORIS, *La lotta al terrorismo*, cit.

[8] In questi termini, M. PANZAVOLTA, *Intercettazioni e spazio di libertà, sicurezza e giustizia*, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, 69.

torare un sistema informatico, rese possibili dall'installazione segreta di uno specifico *software*, c.d. *trojan*[9].

Tale strumento investigativo è emblematico da un lato delle enormi potenzialità che lo sviluppo informatico introduce rispetto alle indagini classiche, dall'altro delle forti tensioni cui esso dà vita rispetto ai diritti fondamentali della persona e alle tradizionali categorie processuali.

Infatti, con un unico strumento è possibile porre in essere diverse attività d'indagine: perquisire l'*hard-disk*, sequestrare i dati rilevanti, intercettare le comunicazioni *VoIP*, attivare le periferiche audio e video per effettuare un'intercettazione ambientale ovvero una videoripresa, rilevare e registrare i siti *web* che vengono visitati, decifrare quel che viene digitato sulla tastiera.

Tale multifunzionalità già di per sé rende evidenti le difficoltà che si incontrano nel tentare di inquadrare le perquisizioni *online* in un'unica categoria. A ciò va aggiunto il fatto che, vertendosi in materia di mezzi di ricerca della prova fortemente limitativi di diritti fondamentali, il primo punto di riferimento dell'interprete non può che essere la cornice costituzionale. Cornice costituzionale che a sua volta si arricchisce di contenuti nuovi. A fronte del progresso tecnologico le garanzie offerte dai tradizionali diritti alla libertà e segretezza delle comunicazioni, all'inviolabilità del domicilio, ma anche da diritti di nuova generazione quali il diritto alla *privacy* o riservatezza, si rivelano insufficienti.

Infatti, nel contesto digitale non ci sono confini, non ci sono luoghi fisici che possano riflettere il carattere privato o riservato delle attività che ivi si svolgano o di ciò che vi sia custodito. La distinzione tra domicilio e altri luoghi di privata dimora da un lato e luoghi riservati dall'altro, utilizzata dalla giurisprudenza in materia di videoriprese, si rivela inadeguata quando applicata ai sistemi informatici. In questo ambito non si riesce più a distinguere tra dati intimi e dati sociali, tra informazioni segrete e informazioni riservate. Un dato apparentemente innocuo, collegato ad altri dati a loro volta apparentemente innocui può in realtà rivelare aspetti della vita di una persona che si desiderano sottrarre alla conoscenza altrui.

[9] Il *trojan* è un programma che installa sul sistema informatico una *backdoor* attraverso cui si crea un collegamento con un *computer* remoto che permette il controllo delle attività che vengono svolte.

Inoltre, una volta effettuato l'accesso ad un sistema informatico, si crea una *porta* – una *backdoor* per l'appunto – da cui possono potenzialmente accedere altri soggetti, diversi dagli investigatori, con conseguente alto pericolo per la sicurezza e l'integrità delle informazioni e dei dati.

Come da tempo evidenziato dalla dottrina penalistica, l'interesse dell'utilizzatore di sistemi informatici è quello alla tutela dei propri dati-informazioni a prescindere dal luogo in cui si trovino o dal mezzo di comunicazione prescelto[10]. Occorre quindi tutelare il sistema informatico in quanto spazio in cui il singolo manifesta la sua personalità, a prescindere dalla natura delle informazioni che vi si affidano[11].

Nasce quindi un nuovo diritto fondamentale, quello alla riservatezza informatica[12]. Tale diritto trova oggi, nel sistema multilivello delle fonti dei diritti, fondamento non solo e non tanto nell'art. 2 Cost.[13], quanto

[10] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di* Internet, Padova, 2004, 80.

[11] R. FLOR, Phishing, identity theft, e identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 899 ss., a cui si deve l'elaborazione della teoria c.d. assiomatica delle sfere di tutela della vita privata, secondo cui all'interno di un sistema informatico non ha più senso distinguere tra sfera individuale e sfera privata, ma occorre prendere atto dell'esistenza di «spazi virtuali di manifestazione della personalità, che coincidono con l'interesse sostanziale alla protezione di informazioni "riservate" e al loro controllo nello svolgimento di rapporti giuridici e personali online o in altri spazi "informatici"».

[12] La riservatezza informatica è definita quale «interesse al godimento e controllo esclusivo sia di determinati dati e informazioni, che dei relativi mezzi e procedimenti informatici e telematici di trattamento, che pur configurandosi sempre quale «diritto di escludere» i terzi non legittimati dal corrispondente accesso e utilizzo, prescinde in tutto o in parte dai tradizionali limiti e presupposti dei concetti civilistici di proprietà o possesso, ovvero dalle condizioni che fondano la rilevanza giuridica del segreto o della riservatezza personale in genere». Così, L. PICOTTI, (voce) *Reati informatici*, in *Enc. giur. Treccani*, agg. VIII, Roma, 2000, 20 ss. Si veda anche R. FLOR, Phishing, identity theft, cit., secondo cui «il bene giuridico "riservatezza informatica", protetto dall'art. 615-*ter* c.p., si può configurare come interesse esclusivo, giuridicamente riconosciuto, di godere, disporre e controllare le informazioni, i procedimenti, i sistemi e "spazi" informatizzati e le relative utilità».

[13] Tale norma secondo l'insegnamento delle Sezioni Unite Prisco, cit., offre le garanzie minime – autorizzazione dell'autorità giudiziaria – per una limitazione legittima

nell'art. 8 CEDU e nell'art. 7 CDFUE. Ai sensi dell'art. 8, par. 2 CEDU e dell'art. 52, co. 1 della Carta, esso potrà essere limitato solo se l'ingerenza è prevista dalla legge – da intendersi come necessità di una base normativa ovvero giurisprudenziale purché uniforme e costante – e nel rispetto del principio di proporzionalità[14].

Come anticipato, a livello europeo, le perquisizioni *online* sono state introdotte per la prima volta nell'ordinamento tedesco, dove poi sono cadute sotto la scure della declaratoria di incostituzionalità nel 2008. In particolare, la Legge sulla protezione della Costituzione del *Land Nord Rhein Westfalen* era stata modificata nel senso di consentire ad un organismo di *intelligence* a "protezione della costituzione" (*Verfassungsschutzbehörde*) lo svolgimento di due tipi di indagini, il monitoraggio e la ricognizione segreti di *Internet* e l'accesso segreto a sistemi informatici. La Corte costituzionale tedesca, chiamata a pronunciarsi sulla legittimità di tale strumento investigativo, ha dichiarato la normativa incostituzionale in quanto non rispettosa dei principi di proporzionalità e determinatezza, ma non ha escluso in assoluto l'ammissibilità di tale strumento[15]. Infatti, di fronte alle sfide lanciate dal progresso tecnologico la Corte ha avvertito l'insufficienza della tutela offerta dai tradizionali diritti fondamentali e la conseguente necessità di creare un nuovo diritto fondamentale, il diritto alla garanzia della segretezza e integrità dei sistemi informatici (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*), considerato una nuova espressione dell'*allgemeines Persönlichkeitsrecht* e della *Menschenwürde* (art. 1, co. 1 e art. 2, co. 1 *Grundgesetz*).

Così delineata la cornice costituzionale di riferimento, il *Bundesverfassungsgericht* ha riconosciuto al legislatore tedesco la possibilità di

---

del diritto alla riservatezza. Garanzie che però non si ritengono sufficienti a fronte dell'uso dello strumento investigativo in esame.

[14] Per un approfondimento sul punto sia consentito rinviare a F. IOVENE, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont. – Riv. trim.*, 3/4, 2014.

[15] *BVerfG*, 27 febbraio 2008, *BVerfGE* 120, 274 ss. Per un commento alla sentenza si veda R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* Online Durchsuchung. *La prospettiva delle investigazioni ad alto contenuto tecnologico e il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, in *Riv. trim. dir. pen. ec.*, 2009, 697 ss.

introdurre, sia per finalità preventive che di repressione dei reati, strumenti investigativi suscettibili di comprimere tale nuovo diritto fondamentale, nel rispetto del principio di proporzionalità e con riserva di giurisdizione. Ha auspicato inoltre l'introduzione di un adeguato sistema di misure tecniche preventive idoneo ad impedire di avere accesso a dati personali, irrilevanti per le indagini o comunque la previsione di garanzie *ex post* consistenti nell'immediata cancellazione di tali dati e nella loro inutilizzabilità processuale.

Le perquisizioni *online* non sono considerate quindi uno strumento da bandire dall'ordinamento, ma un'attività investigativa di cui si riconoscono le enormi potenzialità nella lotta contro gravi forme di criminalità, ma anche l'insidiosità per la riservatezza dei singoli.

Rimanendo in ambito europeo è opportuno segnalare che altri Paesi hanno avviato una riflessione sul tema. In Olanda è stata proposta l'introduzione del c.d. *Trojan* di Stato che consentirebbe alla polizia, su autorizzazione del Giudice, di monitorare l'uso del sistema informatico, copiare i dati in esso contenuti e addirittura distruggerli, se illegali[16].

In Gran Bretagna con il *Serious Crime Act* del 2015 (*Section* 44) è stata modificata la *Clause* 10 (*Savings*) del *Computer Misuse Act* del 1990 ed è stata così riconosciuta una forma di immunità alla polizia che si renda responsabile di un accesso abusivo ad un sistema informatico nell'ambito dell'attività di indagine. La strada scelta non è in questo caso quella dell'introduzione legislativa di un nuovo strumento investigativo, bensì di una speciale causa di giustificazione, ma il risultato finale che si ottiene è sostanzialmente analogo.

Verso fine 2015 in Spagna sono state introdotte le perquisizioni *online* attraverso l'inserimento di specifici articoli nella *Ley de enjuiciamiento criminal* (nuovo capitolo del Libro II, rubricato *Registros remotos sobre equipos informáticos*)[17]. In particolare tale attività investigativa è consentita, per la durata di un mese prorogabile fino ad un massi-

[16] La proposta proviene dal Ministro della Giustizia olandese Ivo Opstelten e risale all'ottobre 2012.

[17] *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*, pubblicata il 6 ottobre 2015, *Boletín Oficial del Estado* n. 239, Sec. I, 90192.

mo di tre mesi, su autorizzazione del giudice, solo nell'ambito di indagini per un catalogo di reati presupposto – criminalità organizzata, terrorismo, delitti contro minori, delitti contro l'ordinamento costituzionale, criminalità informatica –. Si precisa poi che il provvedimento che dispone la misura deve indicare il sistema informatico oggetto di accesso, il modo in cui si eseguirà l'accesso e l'apprensione dei dati, i soggetti autorizzati ad accedere, l'eventuale autorizzazione ad effettuare copia dei dati, le misure tecniche per impedire l'alterazione dei dati, così come per garantire la sicurezza dei dati, ossia evitare l'accesso da parte di terzi e la soppressione[18].

Per quanto riguarda l'Italia, mancano norme che disciplinino specificamente questo strumento investigativo, che solo apparentemente è riconducibile a mezzi di ricerca della prova tipici.

Proprio in sede di conversione del decreto legge in materia di antiterrorismo si era proposta l'introduzione delle perquisizioni *online*. In particolare l'emendamento, poi sparito in sede di conversione definitiva, prevedeva una modifica dell'art. 266 *bis* c.p.p., che riguarda le intercettazioni di comunicazioni informatiche o telematiche, nel senso di consentire

> l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi *anche attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico*.

Seppur si condivida l'opportunità (*rectius*: necessità) di disciplinare questo strumento in via legislativa, posto che disinteressarsi del problema (e lasciare che sia la prassi giurisprudenziale a trovare soluzioni tampone) non è approccio accettabile né soddisfacente, la strada maestra da percorrere non è quella della interpolazione delle norme in mate-

[18] Questo è un punto molto importante nell'ottica della tutela della sicurezza del sistema informatico oggetto di controllo. Infatti, una volta installata la *backdoor* esso si presenta vulnerabile rispetto ad ulteriori accessi, anche da parte di *hackers*.

ria di intercettazioni[19]. Occorre invece introdurre un autonomo articolato normativo che raggiunga un equo bilanciamento, alla luce del principio di proporzionalità, tra diritti costituzionalmente protetti: quello alla riservatezza informatica, da un lato, e quello alla prevenzione e repressione dei reati dall'altro[20].

Analogamente a quanto tradizionalmente previsto per i diritti costituzionali di libertà (artt. 13, 14 e 15 Cost.), eventuali limitazioni del diritto alla riservatezza informatica per finalità investigative dovranno infatti essere subordinate alla doppia riserva di legge e di giurisdizione.

Non si potrà quindi prescindere dalla previsione di un elenco di gravi reati presupposto e dalla necessità di un provvedimento motivato del Giudice su richiesta del Pubblico Ministero. Sarà opportuno disciplinare le modalità dell'intromissione dello svolgimento dell'attività di indagine, prevedendo specifiche garanzie a tutela dei dati personali irrilevanti per le indagini ed apposite sanzioni di inutilizzabilità del materiale probatorio acquisito illegittimamente o irrilevante.

Si dovrebbe inoltre – e ciò acquista particolare importanza nell'ambito del contrasto al terrorismo – stabilire se il ricorso a tale strumento sia consentito anche per finalità preventive.

Infine, per quanto possibile, la disciplina legislativa destinata a durare nel tempo, deve essere "tecnologicamente neutra" in modo da riuscire ad adattarsi ai cambiamenti senza ostacolarli, continuando ad offrire adeguata protezione ai diritti oggetto di tutela. Non è infatti pensabile che le riforme legislative riescano a tenere il passo dell'evoluzione tecnologica, e quindi non ha senso introdurre normative di dettaglio, destinate ad una rapida obsolescenza, ma nemmeno può il legislatore disinteressarsi del fenomeno.

L'assenza di una specifica disciplina legislativa, infatti, comporta il rischio che tale attività rimanga confinata nell'atipicità e che si faccia applicazione dell'art. 189 c.p.p. Questa eventualità è senz'altro da criti-

[19] Soluzione già seguita in sede di ratifica della Convenzione di Budapest sul *Cybercrime* con riguardo alle norme dedicate a ispezioni, perquisizioni e sequestri e che ha originato una serie di problemi applicativi ed interpretativi.

[20] Nel senso dell'opportunità di introdurre un autonomo articolato normativo per disciplinare le indagini ad alto contenuto tecnologico che incidono su diritti fondamentali, si veda anche S. MARCOLINI, *Le indagini atipiche*, cit.

care poiché non bisogna dimenticare che il primo requisito di validità della prova atipica è la sua legittimità costituzionale[21], e non pare che allo stato le perquisizioni *online* superino questo vaglio. Infatti, come già messo in evidenza, simile poliedrico strumento investigativo è suscettibile di ledere a più livelli la sfera privata della persona.

Come anticipato, nell'inerzia del legislatore, a fronte delle esigenze che emergono nella prassi soprattutto nell'ambito delle indagini in materia di criminalità organizzata di stampo mafioso, la giurisprudenza ha svolto il consueto, ma improprio, ruolo di supplenza.

Recentemente, infatti, le Sezioni Unite della Cassazione sono state chiamate a pronunciarsi sulla ammissibilità delle c.d. intercettazioni a mezzo *trojan*, ossia delle intercettazioni ambientali rese possibili dall'installazione di tale *software* di indagine su un dispositivo informatico – *smartphone*, *tablet* o *pc* – e conseguente attivazione delle periferiche audio[22].

La Sezione VI, con sentenza del 26 maggio 2015 aveva ritenuto inammissibile tale forma di intercettazione in quanto consentiva di captare le conversazioni in qualsiasi luogo si recasse il soggetto portando con sé l'apparecchio intercettato. Ciò doveva ritenersi non consentito dall'art. 15 Cost., che essendo norma di stretta interpretazione esigeva

[21] In questo senso si sono pronunciate le Sezioni Unite Prisco, cit., nell'esaminare la questione dell'ammissibilità, in mancanza di una disciplina positiva *ad hoc*, di videoriprese di comportamenti non comunicativi all'interno del domicilio. Secondo la Suprema Corte, infatti, non veniva in rilievo in questo caso il tema della prova incostituzionale perché «prima dell'ammissione le prove atipiche non sono prove, perciò se sorge questione sulla legittimità delle attività compiute per acquisire i materiali probatori che le sorreggono ci si deve interrogare innanzitutto sulla loro ammissibilità, piuttosto che sulla loro utilizzabilità […]»; presupposto di ammissibilità di una prova atipica è che si tratti di un'attività "non disciplinata dalla legge", con questa espressione, proseguono le Sezioni Unite, «il codice si riferisce immediatamente alla mancanza di una disciplina che concerna sotto l'aspetto processuale la prova da assumere, ma è anche vero che non può considerarsi "non disciplinata dalla legge" la prova basata su un'attività che la legge vieta». E un'attività di indagine che comporti un'intromissione in diritti fondamentali, tutelati dalla Costituzione con doppia riserva di legge e di giurisdizione, in assenza di una disciplina specifica, è un'attività che la legge vieta.

[22] Cass., Sez. Un., 28 aprile 2016, n. 26889.

che l'intercettazione ambientale dovesse avvenire in luoghi ben circoscritti ed individuati *ab origine*.

La stessa Sezione in diversa composizione, non condividendo questo orientamento, ha invece affermato che il riferimento al luogo è funzionale alle modalità esecutive dell'intercettazione di tipo "tradizionale", che avviene per mezzo della collocazione fisica di microspie, ma che tuttavia

> il principio secondo cui il decreto deve individuare con precisione i luoghi in cui dovrà essere eseguita l'intercettazione delle comunicazioni tra presenti non solo non è desumibile dalla legge, ma, […] non risulta essere stato mai affermato dalla giurisprudenza e, inoltre, non sembra costituire un requisito significativo funzionale alla tutela dei diritti in gioco (artt. 14, 15 Cost. e 8 CEDU) [23].

La rimessione alle Sezioni Unite nasceva quindi da un contrasto giurisprudenziale rispetto alla necessità che il decreto autorizzativo di intercettazioni ambientali tramite *software trojan* dovesse o meno indicare i luoghi in cui la captazione doveva avvenire, in particolare nel caso un cui l'intercettazione fosse disposta nell'ambito di delitti di criminalità organizzata.

Le Sezioni Unite con sentenza depositata il primo luglio dello scorso anno hanno ammesso il ricorso a tale intercettazione ambientale tramite *trojan* anche se i luoghi non sono preventivamente individuati nel decreto autorizzativo e quindi anche in luoghi di privata dimora pur se ivi non si stia svolgendo l'attività criminosa, ma solo limitatamente ai procedimenti relativi a delitti di criminalità organizzata, anche terroristica (ossia quelli elencati nell'art. 51, co. 3 *bis* e 3 *quater* c.p.p.), nonché quelli comunque facenti capo ad un'associazione a delinquere, escluso il concorso di persone nel reato.

Infatti, in deroga al disposto di cui all'art. 266, co. 2 c.p.p., l'art. 13 d.l. 152/1991 convertito in legge 203/1991 non richiede, laddove si tratti di indagini in materia di criminalità organizzata come ulteriore presupposto per l'intercettazione nei luoghi di cui all'art. 614 c.p. che vi sia motivo di ritenere che ivi si stia svolgendo l'attività criminosa. Ciò

[23] Cass., Sez VI., ord. 10 marzo 2016, n. 13884.

significa che il decreto autorizzativo delle intercettazioni non deve necessariamente indicare i luoghi in cui si svolgerà l'attività captativa, e quindi che le intercettazioni ambientali tramite *trojan* sono pienamente ammissibili.

Non è questa la sede per un commento a tale sentenza, ma pare potersi fin d'ora sostenere che si tratta di una soluzione di compromesso che da un lato non priva gli investigatori di un importante strumento nella lotta contro gravi forme di criminalità organizzata, e dall'altro, nella consapevolezza della diversità di questa forma di intercettazione ambientale itinerante rispetto alle modalità classiche delle intercettazioni ambientali, non forza il dettato legislativo.

Alla luce di questo quadro giurisprudenziale non si può che ribadire la necessità – e l'urgenza – dell'intervento del legislatore.

## *4.* Data retention

La tensione tra esigenze di sicurezza e repressione penale da un lato e diritti fondamentali dall'altro si avverte anche con riferimento ad un altro strumento, all'apparenza meno invasivo, quale la conservazione e successiva acquisizione di dati di traffico telematico (e telefonico), c.d. *data retention*.

La Corte di giustizia dell'Unione europea ha recentemente – e correttamente – affermato che tale attività costituisce una limitazione del diritto al rispetto della vita privata e di quello alla tutela dei dati personali, garantiti rispettivamente dagli artt. 7 e 8 CDFUE[24].

Infatti, benché non si apprenda il contenuto della comunicazione, tali dati consentono di ottenere informazioni sulla vita privata di una persona, creare profili della personalità, tracciare i movimenti degli utenti:

[24] Corte di giustizia dell'Unione europea, 8 aprile 2014, cause riunite C-293/12, C-594/12. Per un primo commento della sentenza si veda E. COLOMBO, "Data retention" *e Corte di giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.*, 2014, 2705 ss.; e R. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d.* "data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *www.penalecontemporaneo.it*, 28 aprile 2014.

destinatario, data, ora, luogo, orario di una comunicazione, siti *Internet* visitati permettono, se combinati tra loro, e se la conservazione riguarda un lasso apprezzabile di tempo, di ottenere dettagliate informazioni ad esempio sulle relazioni sociali o sulle inclinazioni personali, costituendo senza dubbio un'ingerenza nel diritto alla riservatezza della vita privata[25]. Ingerenza che si giustifica solo se, ai sensi dell'art. 52, co. 1 CDFUE, è prevista dalla legge, rispetta il nucleo essenziale di tali diritti ed è proporzionata all'obiettivo da raggiungere, corrispondente o a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Sulla base di tali premesse, la Corte di giustizia ha eseguito un *test* di proporzionalità della direttiva c.d. *data retention*[26], concludendo poi per la sua invalidità.

In particolare la Corte di giustizia ritiene necessaria già in fase di raccolta dei dati una delimitazione degli scopi della conservazione. Ciò sulla base della corretta considerazione che il diritto al rispetto della vita privata e il diritto alla tutela dei dati personali vengono lesi due volte, dapprima per effetto della raccolta e conservazione dei dati e successivamente al momento dell'acquisizione. Si tratta di una forma di tutela molto avanzata di tali diritti, ma altrettanto evidente è il sacrificio delle esigenze investigative, oltre alla difficoltà tecnica di realizzare simile obiettivo.

---

[25] Cfr. *BVerfG*, 2 marzo 2010, *1BvR 256/08*, *1 BvR 263/08*, *1 BvR 586/08*, reperibile anche su *www.bundesverfassungsgericht.de*.

[26] Direttiva 2006/24/CE. La storia della direttiva *data retention* è stata fin dall'origine travagliata; innanzitutto ne era stata contestata la base giuridica poiché trattandosi di un atto preordinato ad agevolare l'indagine, l'accertamento e la repressione dei reati si riteneva che fosse un atto di Terzo Pilastro e quindi che si sarebbe dovuta adottare una decisione quadro. La Corte di giustizia ha invece ritenuto legittima la scelta operata (C. giust. CE, sentenza 10 febbraio 2009, causa C-301/06, Irlanda c. Parlamento e Consiglio, in *www.curia.eu*). Inoltre, la normativa nazionale di recepimento della direttiva è stata dichiarata incostituzionale in quattro Paesi Membri, Romania (8 ottobre 2009), Bulgaria (11 dicembre 2008), Germania (2 marzo 2010) e Repubblica Ceca (31 marzo 2011). Cfr. R. FLOR, Data retention *e limiti al potere coercitivo dello Stato in materia penale: le sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională, in *Cass. pen.*, 2011, 1952 ss.

Inoltre, si finirebbe in questo modo per sovrapporre la *data retention* al *data freezing*, che invece consiste proprio nella possibilità per l'autorità giudiziaria, una volta che un reato è già stato commesso, di ordinare la conservazione dei dati di traffico.

Più convincente la ricostruzione fatta dalla Corte costituzionale tedesca nella sentenza con cui nel 2010 ha dichiarato incostituzionale la normativa nazionale di recepimento della direttiva *data retention*[27]. Infatti, la Corte ha creato un forte collegamento tra conservazione e acquisizione, in forza del quale pur essendo la conservazione indiscriminata, essa può considerarsi legittima se l'acquisizione di quei dati può avvenire solo per scopi specifici e determinati.

La Corte di giustizia esige inoltre la predisposizione di criteri oggettivi volti a delimitare l'accesso delle competenti autorità nazionali ai dati e al loro uso a fini di prevenzione, accertamento o indagine con riferimento a reati che possano, quanto alla portata e alla gravità dell'ingerenza nei diritti fondamentali, considerarsi sufficientemente gravi; la previsione di specifiche modalità di accesso ed in particolare di una forma di controllo da parte di un Giudice o comunque di un'entità amministrativa indipendente; ed infine misure tecniche per garantire la sicurezza e la protezione dei dati, in modo da prevenire eventuali accessi abusivi ed usi illeciti dei dati stessi.

Si tratta di un punto particolarmente delicato, che coinvolge il più ampio tema del ruolo sempre più importante che i privati, nel caso di specie gli *Internet Service Providers*, assumono nell'ambito delle indagini penali. Infatti, i costi della conservazione sono addossati ai *providers*, ciò che, come è stato acutamente evidenziato, ha probabilmente determinato la fortuna di questo strumento di indagine[28]. Non bisogna dimenticare tuttavia che i *providers* sono imprenditori che operano secondo le regole del mercato e quindi con criteri di economia, non necessariamente sintomo di alti *standards* di sicurezza.

---

[27] *BVerfG*, 2 marzo 2010, cit.

[28] M.A. ZÖLLER, *Die Vorratsspeicherung von Telekommunikationsdaten – (Deutschen) Wege und Irrwege*, *Congress on the Criminal Law Reforms in the World and in Turkey. Atti del convegno internazionale svoltosi a Istanbul-Ankara dal 26 maggio al 4 giugno 2010*, Istanbul, 2010, 33.

L'Italia ha recepito la direttiva *data retention* nel 2008 (d.lgs. 109/2008) attraverso una modifica dell'art. 132 codice *privacy*, che oggi prevede un obbligo per i gestori di servizi di telecomunicazione di conservazione, escluso il contenuto della comunicazione, dei dati di traffico telefonico per 24 mesi, di quelli di traffico telematico per 12 mesi e di quelli relativi alle chiamate senza risposta per 30 giorni per finalità di accertamento e repressione dei reati.

La declaratoria di invalidità della direttiva non comporta automaticamente l'invalidità della normativa attuativa, ma, venuto meno il diritto secondario, occorre verificare la compatibilità del diritto interno con il diritto primario dell'Unione, e quindi con i diritti fondamentali di cui agli artt. 7, 8 e 52 CDFUE. Vaglio che va condotto alla luce dei criteri fissati dalla Corte di giustizia[29].

Non sembra che l'art. 132 codice *privacy* superi tale vaglio. Infatti, tale norma non pone alcun limite, oltre a quello strettamente temporale, alla conservazione dei dati; non limita a particolari forme di criminalità l'uso di tali dati; non prevede specifiche modalità di accesso, né richiede il vaglio di un Giudice o di altra autorità indipendente[30]; non prevede particolari misure per la sicurezza dei dati[31].

Di tale situazione il legislatore italiano non si è ad oggi mostrato consapevole. L'unico intervento legislativo che coinvolge in senso ampio l'art. 132 codice *privacy* è contenuto proprio nella legge anti-

[29] Sul punto sia consentito rinviare a F. IOVENE, Data retention *tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 2014, 4274 ss.

[30] Nonostante la particolare posizione ricoperta dal Pubblico Ministero nel nostro ordinamento, non bisogna dimenticare che si tratta pur sempre di una parte, ancorché pubblica, e quindi di un soggetto non terzo rispetto alle indagini.

[31] Il Garante per la *Privacy*, con provvedimento del 17 gennaio 2008 è intervenuto per dettare dei criteri per garantire la sicurezza dei dati conservati, quali dotarsi di idonei strumenti di autenticazione e autorizzazione, conservare separatamente i dati di traffico utilizzati per finalità di accertamento e repressione dei reati rispetto a quelli utilizzati per altre finalità, cancellare i dati decorsi i termini massimi di conservazione, approntare strumenti in grado di permettere il controllo delle attività svolte sui dati da ciascun incaricato, e utilizzare sistemi di cifratura e protezione dei dati. Si tratta tuttavia di un atto di *soft law*, privo di efficacia vincolante. Provvedimento pubblicato in G.U. del 5 febbraio 2008, n. 30.

terrorismo dell'aprile 2015[32]. Viene introdotto un regime parzialmente derogatorio circa i tempi di conservazione dei dati di traffico telefonico e telematico che possono essere usati ai fini delle indagini per i reati di terrorismo (di cui agli artt. 51, co. 3 *quater* e 407, co. 2 lett. a) c.p.p.). Si prevede infatti che in relazione ai procedimenti per tali reati, dalla data di entrata in vigore della legge di conversione, i dati relativi al traffico telefonico, telematico e alle chiamate senza risposta effettuati a partire da quella stessa data vengano conservati fino al 31 dicembre 2016 (art. 4 *bis*). Si tratta di una norma temporanea, espressamente destinata a perdere efficacia a partire dal primo gennaio 2017, la cui *ratio* sfugge.

In virtù della primazia e dell'effetto diretto del diritto primario europeo, in attesa di un doveroso intervento legislativo, il giudice nazionale dovrebbe quindi disapplicare tale norma nel caso concreto, con conseguente inutilizzabilità *ex* art. 191 c.p.p. dei dati così acquisiti[33].

Si tratta di una conclusione che presenta evidentemente i limiti dell'essere un rimedio legato al caso concreto, destinato ad operare *ex post*, quando ormai la violazione dei diritti fondamentali si è verificata e che non risolve il problema della conservazione e acquisizione per finalità di *intelligence*.

## *5. Conclusioni*

L'effettività di un'efficace lotta contro gravi forme di criminalità dipende sempre più frequentemente dall'uso di strumenti di indagine ad alto contenuto tecnologico. In questo contesto è particolarmente avvertita la necessità di una sinergia tra informatica e diritto: solo un'adeguata comprensione del funzionamento dei sistemi informatici e degli strumenti di *computer forensics* permette infatti di apprestare idonee garanzie a tutela dei diritti fondamentali. Compito del diritto è quindi quello

[32] D.l. 19 febbraio 2015, n. 41, convertito con modifiche in l. 17 aprile 2015, n. 43, pubblicato sulla G.U. del 20 aprile 2015, n. 91.

[33] Si tratta infatti senz'altro di materia che rientra in quelle di competenza dell'Unione, rispetto alla quale si deve fare applicazione dei principi generali del diritto europeo.

di aggiornare, attraverso l'evoluzione normativa e giurisprudenziale, le tradizionali categorie concettuali in modo da non lasciare i singoli sprovvisti di tutela.

Conciliare regole tecniche e regole giuridiche non è facile. Ne è un ulteriore esempio il tema del sequestro preventivo di siti *web*. Sia le Sezioni Unite della Cassazione[34] che il Legislatore proprio nella legge anti-terrorismo (art. 2, co. 4) hanno affermato a chiare lettere che lo strumento per oscurare il contenuto dei siti *web* è quello del sequestro preventivo, con ciò superando le perplessità di chi vedeva un ostacolo nelle diverse modalità con cui il sequestro viene eseguito. Il sequestro preventivo è infatti una tipica misura ablatoria, mentre il sequestro di siti *web* si traduce in una misura inibitoria rivolta al fornitore di connettività che deve impedire agli utenti l'accesso al sito o alla singola pagina *web* incriminati ovvero rimuovere il *file* che viene in rilievo; si tratta quindi di un obbligo di *facere*.

Resta però aperto il problema di come materialmente effettuare il sequestro, posto che l'art. 321 c.p.p., diversamente dall'art. 254 *bis* c.p.p. che disciplina il sequestro probatorio di dati presso fornitori di servizi – e che è stato introdotto in sede ratifica della Convenzione *Cybercrime* – è muto circa le modalità, la cui individuazione sembra, ancora una volta, affidata ai *service providers* stessi. Inoltre, l'inibitoria proveniente dall'autorità giudiziaria italiana è coercitiva solo rispetto ai *providers* nazionali e ha un ambito di applicazione territorialmente limitato, che si pone in frizione con la ontologica transnazionalità di *Internet*, con la conseguenza che il sito risulterà *oscurato*, ossia inaccessibile solo per gli utenti che accedono da un determinato territorio, con indirizzo *IP* localizzabile[35].

[34] Cass., Sez. Un., 29 gennaio 2015, n. 31022.

[35] Ad eccezione delle ipotesi in cui esistono strumenti di cooperazione giudiziaria. Ad esempio, la direttiva 2011/92/UE in materia di lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile prevede all'art. 25 che gli Stati membri adottino «le misure necessarie per assicurare la tempestiva rimozione delle pagine *web* che contengono o diffondono materiale pedopornografico ospitate nel loro territorio e si *[adoperino]* per ottenere la rimozione di tali pagine ospitate fuori dal loro territorio». Gli strumenti di contrasto previsti hanno quindi come ambito di applicabilità l'intero territorio UE.

Le innovazioni tecnologiche offrono senza dubbio un importante strumento per la lotta contro la criminalità. Come evidenziato, tale strumento si rivela particolarmente invasivo dei diritti fondamentali della persona. Diritti fondamentali che, nel rispetto del loro nucleo essenziale, e del principio di proporzionalità, sono tuttavia limitabili in un'ottica di bilanciamento con altrettanto fondamentali esigenze di contrasto alla criminalità.

Pertanto, la soluzione auspicabile non è quella di bandire dall'ordinamento determinate tecniche investigative, ma di disciplinarle puntualmente.

# QUARTA SESSIONE

# QUALE DIRITTO PENALE NELLA DIMENSIONE GLOBALE DEL *CYBERSPACE*?

*Lorenzo Picotti*

1. Nel dare inizio alla quarta ed ultima sessione di lavori, non posso non ringraziare cordialmente gli organizzatori Gabriele Fornasari e Roberto Wenin, per l'invito a presiederla. Invito particolarmente gradito e significativo, perché qui a Trento ho insegnato per otto anni, avendo iniziato quando ricorreva il decimo anniversario di fondazione della Facoltà di Giurisprudenza, ed oggi già ne festeggiamo il trentennale. Ma mi sento sempre tra amici, e l'impressione è che non sia passato tutto questo tempo, specie stando in quest'aula, in cui ho tenuto tante lezioni e si sono svolti tanti Convegni, ai quali questo si aggiunge senz'apparente soluzione di continuità. Al riguardo ricordo come, proprio in quegli anni, precisamente nel 2000 – alla svolta del secolo o, se vogliamo essere enfatici, del millennio! – il Preside Roberto Toniatti mi chiese se ero disponibile a tenere un nuovo corso d'insegnamento facoltativo, dai contenuti specialistici, accanto a quelli tradizionali di diritto penale: quello di "diritto penale dell'informatica", che si sarebbe affiancato ad un altro che parallelamente avrebbe tenuto il collega Vanni Pascuzzi sul "diritto privato dell'informatica". Accolsi con entusiasmo la proposta. E la Facoltà approvò l'inserimento dei due corsi nel piano degli studi. L'insegnamento venne dunque attivato con un programma iniziale che definirei sperimentale, ma che si arricchì poi, nel corso degli anni, di contenuti e novità, suscitando crescente interesse, partecipazione ed impegno da parte degli studenti. Devo dire che fu una scelta lungimirante, che precorreva i tempi. E lo stimolo fu davvero importante anche per me, perché mi consentì di raccordare strettamente lo sviluppo della ricerca scientifica (che avevo da tempo iniziato ad indirizzare anche su questa specifica branca) con quello della didattica, aggiornata costantemente per contribuire a formare, nel modo migliore

possibile, giuristi e studiosi aperti alla "modernità", come, per l'appunto, suggerisce l'argomento dell'odierno convegno. Ne sia concreta conferma il fatto che oggi ho qui al mio fianco, al tavolo dei relatori, due cari e valenti allievi trentini di allora, Roberto Flor ed Ivan Salvadori, che dopo aver seguito quel corso, si sono brillantemente laureati con tesi in diritto penale dell'informatica, di cui sono stato relatore, e che poi mi hanno seguito nella sede veronese, nella quale hanno conseguito il dottorato di ricerca, approfondendo e sviluppando proprio detti filoni di indagine, ai quali si sono proficuamente dedicati anche nei successivi percorsi di studio ed accademici, che mi auguro possano presto offrir loro tutte le soddisfazioni che meritano.

2. Vengo dunque ad introdurre i nostri lavori. Allora vivevamo il passaggio dal *Computer-crime* al *Cybercrime*, effetto dell'apertura di Internet al pubblico, della "rete delle reti" resa accessibile a tutti: il *world wide web*[1]. Certo, il *Cyberspace* non era ancora così pervasivo, non c'erano ancora i *social network*, i *tablet*, il *cloud*, gli *smartphone*. Però i problemi giuridici essenziali già si profilavano con nitidezza, non essendoci più soltanto da fronteggiare la criminalità informatica che si manifestava su computer *stand alone* ovvero infettando singoli supporti, come i *floppy disk*, o tutt'al più aggredendo il contesto chiuso di reti interne di enti ed aziende: emergeva invece la necessità di contrastare – con ulteriori specifiche incriminazioni, laddove non bastasse l'interpretazione evolutiva delle fattispecie esistenti – i c.d. reati *cibernetici*, quali gli attacchi informatici in rete, gli accessi abusivi da remoto, le frodi per via telematica, le falsità e manipolazioni a distanza di dati di rilevanza probatoria e documentale, anche a prescindere dalla loro stabile connessione con un determinato supporto fisico, la diffusione incontrollata di materiali illeciti (dalla pedopornografia, alla propaganda razzista e nazista, dalle opere musicali e cinematografiche o comunque digitali abusivamente riprodotte, ai dati personali e sensibili trattati in violazione del consenso degli interessati e della specifica disciplina in materia,

[1] Cfr. gli atti del nostro primo convegno trentino in argomento: L. PICOTTI (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, in specie già nella Presentazione, p. VII.

ecc.). E non si ponevano solo concrete questioni ermeneutiche o concernenti le tecniche di formulazione normativa delle nuove fattispecie, ma anche altre più generali, riguardanti in particolare i presupposti ed i limiti della responsabilità (anche penale) degli *Internet Service Providers*[2], correlata al loro ruolo sempre più importante nello sviluppo e nella gestione della rete ed, appunto, dei «servizi della società dell'informazione» – per usare la terminologia europea – fino al loro coinvolgimento nelle indagini, nella ricerca e nell'acquisizione delle prove di reati ed attività illecite. Proprio sul versante processuale emergeva, infatti, la necessità di nuovi strumenti e regole in materia di "prove elettroniche", che ne assicurasse anche la successiva "circolazione" ed utilizzabilità oltre i singoli confini nazionali, con un'armonizzazione indispensabile per sviluppare la cooperazione giudiziaria e di polizia fra Stati diversi, salvaguardando nel contempo, con adeguate garanzie condivise, i diritti fondamentali delle persone non solo nel processo, ma più in generale nella stessa rete.

Il tema si saldava dunque – e si salda ancor oggi – con altri propri della "modernità": a partire da quello dei rapporti fra diritto penale e globalizzazione, fino a quello più specifico del "diritto penale europeo", su cui pure ci impegnammo approfonditamente in quegli anni, con ricerche, pubblicazioni scientifiche e convegni, parimenti organizzati nella Facoltà trentina[3].

Intreccio di argomenti che dunque caratterizzava e caratterizza tuttora le "sfide" al diritto penale poste dall'impetuoso sviluppo tecnologico, proprio perché esso interagisce costantemente e si confonde con quello sociale, economico, politico.

---

[2] Sia consentito rinviare a miei due specifici contributi in materia di quel periodo: L. PICOTTI, *Fondamento e limiti della responsabilità penale dei Service-providers in* Internet, in *Diritto penale e processo*, 1999, n. 3, 379 s.; ID., *La responsabilità penale dei* Service-providers *in Italia*, *ivi*, n. 4, 501 s.

[3] Cfr. L. PICOTTI (cur.), *Il* Corpus Juris *2000. Nuova formulazione e prospettive di attuazione*, Padova, 2004, che raccoglieva gli atti dell'omonimo convegno, avente ad oggetto il testo proposto all'esito dell'articolato studio comparato (c.d. *Suivi*) coordinato da M. DELMAS-MARTY, J.A.E. VERVAELE (éds.), *La mise en oeuvre du Corpus Juris dans les états Membres. Dispositions pénales pour la protection des Finances de l'Europe*, voll. I-IV, Antwerpen-Groningen-Oxford, 2000-2001.

In breve: la progressiva dislocazione *on line* o, meglio, nel *Cyberspace* di una gran parte dei rapporti personali, economici, politici e giuridici, ha trasferito nella rete anche quelli illeciti ed, in particolare, i conflitti d'interessi e le "offese" di quelli meritevoli di protezione, richiedendo un pronto adeguamento delle risposte giuridiche e penali a questo nuovo modo di configurarsi della realtà sociale, per prevenire e possibilmente ricomporre i conflitti stessi, proteggendo i beni – anche del tutto nuovi – nascenti da detto sviluppo, che appaiono non meno meritevoli e bisognosi di tutela penale rispetto a quelli tradizionali.

3. Alla luce di tale sviluppo, la domanda preliminare alla quale si deve dare risposta, nell'odierna sessione di lavori – dopo le bellissime sessioni precedenti, ricche di analisi, riflessioni, spunti critici e prospettive anche molto concrete – è *se* il diritto penale, ma vorrei dire il diritto in quanto tale, possa realmente governare la complessità di Internet e della rete, in tutte le sue varie e mutevoli articolazioni e nella sua perenne e rapidissima evoluzione, in quanto realtà globale estremamente dinamica, non solo tecnologica, ma anche o prima di tutto "sociale". Si potrebbe precisare così la questione: *se* il diritto possa avere un ruolo ed uno spazio propri nel *Cyberspace*, in grado di affermare ed imporre regole dotate di legittimazione ed effettività, nonostante il dominio, che appare totale, della dimensione tecnologica e dei meri rapporti di fatto (o di forza) che con essa si possono stabilire, mediante controlli capillari e sotterranei attacchi, nonché corrispondenti contromisure, in mano di organizzazioni spesso occulte o d'*intelligence*, pubbliche e private, coinvolte in un incessante "conflitto cibernetico" nel quale il singolo individuo, la *persona* con i suoi diritti ed interessi, sembra schiacciata ed inerme.

Come giurista, ritengo che si debba dare una convinta risposta *affermativa* a tali domande, muovendo dal rilievo che il diritto ha storicamente e politicamente proprio la funzione di regolare i rapporti sociali, in un modo pubblicamente "prevedibile" e sulla base di un consenso democraticamente espresso, che ne legittimi le fonti di produzione, risolvendo i conflitti fra gli interessi contrapposti per proteggere quelli meritevoli e bisognosi di effettiva tutela, di fronte ad ogni prevaricazio-

ne ed offesa. Solo così può preservarsi l'ordine *giuridico*, di cui vi è un bisogno non meno forte nell'odierna società globalizzata, proprio per l'interdipendenza strutturale delle sue molteplici componenti, che superano i confini nazionali, richiedendo il *rafforzamento* degli strumenti di regolazione e coesione, capaci di garantire al livello più elevato ed efficace possibile la pacifica convivenza (da cui dipende anche la possibilità d'estensione dei mercati e degli scambi), non certo il loro abbandono o dissolvimento.

In altri termini: anche nel *Cyberspace* servono regole *giuridiche* riconoscibili e condivise, dotate di efficacia e suscettibili di applicazione coattiva, in ipotesi di mancata adesione o rispetto da parte dei destinatari, con ricorso, dunque, anche a mezzi sanzionatori formali e coercitivi, riservati ad autorità e giudici imparziali, in conformità ai principi dello Stato di diritto.

Per questo occorre dedicare studio ed impegno, come queste giornate di lavori dimostrano, per individuare i punti nodali su cui intervenire, per adeguare e rafforzare – sulla base di documentate analisi e ponderate valutazioni – non solo le norme, comprese quelle penali, ma anche le tecniche e gli strumenti di controllo ed accertamento, rispondendo nel modo più efficace e specifico possibile alle necessità di tutela che emergono nel *Cyberspace*, senza sacrificare, ma anzi dando pieno riconoscimento anche in questo nuovo contesto alla protezione dei diritti fondamentali, di cui sono al contempo oggetto e limite.

Il tema della lotta al *terrorismo* internazionale – da combattere anche in rete o, addirittura, a partire dalla rete – con strumenti giuridici e penali (e certo anche d'*intelligence*, come pure politici e culturali), in un contesto di massima armonizzazione e cooperazione sovranazionale, rappresenta un ambito paradigmatico per saggiare i nuovi strumenti di intervento preventivo e repressivo, valutandone contenuti e limiti alla stregua delle più recenti riforme. In questo campo sono infatti messe drammaticamente ed emblematicamente in evidenza le tensioni e frizioni di fondo fra l'esigenza di anticipazione estrema delle soglie di rilevanza penale delle condotte e degli atti oggetto d'incriminazione, da un lato, per consentire l'immediato attivarsi dei mezzi d'indagine più sofisticati e dei poteri coercitivi cautelari, al fine di evitare il realizzarsi od il ripetersi di fatti atroci e sanguinosi, adempiendo nel modo più ef-

ficace possibile alla funzione di prevenzione generale e speciale; e le garanzie della persona, dall'altro, da salvaguardare comunque, in uno Stato di diritto, perché indispensabili per la legittimità stessa del ricorso alla forza coercitiva della pena e degli strumenti propri del sistema penale.

4. Il confronto giuridico su questi temi non può che muovere dalle diverse istanze sovranazionali, rappresentate in particolare da Nazioni Unite, Consiglio d'Europa, Unione europea.

Abbiamo fonti che vincolano i legislatori ed i giudici nazionali, seppur con diversa intensità e portata, da non considerare soltanto in termini negativi di limitazioni della sovranità e della discrezionalità politico-criminale degli Stati, ma anche positivi di formidabile rafforzamento della comune azione, per raggiungere obiettivi condivisi, da correlare a meccanismi più avanzati, seppur complessi, di garanzia giuridica, adeguati alla realtà globale e sovranazionale che abbiamo di fronte.

Il superamento della dimensione nazionale non deve cioè significare rinuncia ai principi garantisti del diritto penale ed, a monte, del sistema di democrazia da cui essi scaturiscono: ma non possiamo, però, neppure restare ancorati ad una nozione di legalità intesa nei termini nazionalistici in cui poteva essere concepita, seppur magistralmente, da Beccaria nell'epoca dell'Illuminismo[4], facendola rigidamente coincidere con la riserva assoluta di legge *statale*.

Le fonti di produzione del diritto anche penale oggi si articolano, alla stregua della nostra stessa Costituzione, in una pluralità di livelli, che interagiscono e devono reciprocamente compenetrarsi, per poter rispondere alle complesse esigenze della difesa sociale in un'ormai necessaria dimensione transnazionale. Accanto all'art. 25, comma 2, Cost., bisogna considerare anche gli artt. 11, 12 e 117 Cost., che consentono ed anzi impongono limitazioni di sovranità e riconoscono

[4] Ci si consenta di rinviare al riguardo ai contributi raccolti in L. Picotti (cur.), *Alle radici del diritto penale moderno: l'illuminismo giuridico di Cesare Beccaria di fronte al potere di punire* (Atti della sessione penalistica del Convegno "Attualità e storicità di «Dei delitti e delle pene» a 250 anni dalla pubblicazione" - Verona, 24 ottobre 2014), Napoli, 2015.

espressamente i vincoli derivanti dagli obblighi sovranazionali, operanti anche per la materia penale, al fine di assicurare «la pace e la giustizia fra le Nazioni».

Del resto, la democraticità di questo articolato sistema di fonti è salvaguardata non solo dal fatto che è il Parlamento nazionale che interviene per la ratifica ed attuazione delle Convenzioni internazionali, ma anche dal suo ruolo di controllo attivo nella fase ascendente del processo legislativo dell'Unione europea in materia penale, in cui l'ultima parola spetta comunque sempre al Parlamento europeo, mentre quelli nazionali vigliano sul rispetto dei principi di sussidiarietà e di proporzione ed hanno facoltà d'azionare il c.d. freno d'emergenza, se vengano in gioco principi fondamentali dei loro ordinamenti, vedendosi in ogni caso affidata, nella fase discendente, l'attuazione concreta delle direttive europee, vincolanti sugli obiettivi da raggiungere, non sui modi e mezzi per conseguirli. Se poi si considera il controllo giudiziario della Corte di giustizia dell'Unione europea su tutti gli atti riconducibili allo «spazio di libertà, sicurezza e giustizia» a partire dal pieno rispetto dei Trattati, cui è assimilata la Carta dei diritti fondamentali dell'Unione (*ex* art. 6 TUE), e quello delle Corti costituzionali nazionali, che possono far valere "controlimiti" interni alla primazia del diritto europeo, quando vengano in gioco diritti e principi fondamentali dell'ordinamento, non può davvero ritenersi che le garanzie dello Stato di diritto siano venute meno, restando altresì sempre assicurato il ricorso individuale alla Corte europea dei diritti dell'uomo contro le violazioni della Convenzione del 1950 e dei suoi protocolli addizionali.

Il giurista ha in definitiva a disposizione un complesso molto ricco di principi, norme fondamentali "giustiziabili", istanze di controllo da valorizzare, per tracciare i possibili nuovi percorsi e limiti di una legislazione penale armonizzata ed equilibrata, in grado di dar risposta ai fenomeni da contrastare su scala sovranazionale, e per sindacare l'operato della giurisprudenza, nella consapevolezza che sia quella europea, sia quella interna, lungi dallo sgretolare la legalità penale, possono dare un contributo fondamentale all'applicazione coerente ed efficace delle singole disposizioni, alla luce del quadro sovranazionale, in particolare modo grazie al metodo dell'interpretazione conforme, che consente di

superare le possibili discrasie fra i diversi livelli di produzione del diritto secondo priorità verificabili.

In questo processo, il formante dottrinale ha un ruolo molto importante, come possiamo constatare nell'esperienza degli ultimi anni, in quanto promuovendo da tempo, con il metodo della comparazione giuridica, il dialogo fra i diversi ordinamenti, può sviluppare i criteri per una sistemazione coerente del menzionato "pluralismo delle fonti" ed offrire le indispensabili basi concettuali e dogmatiche per l'ulteriore sistemazione ed elaborazione normativa e giurisprudenziale, controllandone criticamente (come è suo compito) gli orientamenti. Il nostro ruolo di studiosi non è quindi inutile o marginale, benché sia più complesso e meno delimitato da parametri circoscritti e definiti, come quelli d'un tempo. Ed è questo l'insegnamento che va trasmesso alle nuove generazioni di giuristi, che abbiamo il dovere di formare nel nuovo contesto.

5. Tornando ai contenuti specifici della nostra sessione, il campo del *diritto penale dell'informatica* sembra emblematico per tracciare l'evoluzione, cui abbiamo assistito di persona in pochi decenni.

Dopo il primo emergere delle necessità di tutela giuridico-penale contro la criminalità "da computer" che iniziava a manifestarsi fin da prima degli anni Ottanta dello scorso secolo negli Stati Uniti ed in altri Paesi tecnologicamente avanzati, come la Germania in ambito europeo, si è assistito non solo allo sviluppo di interpretazioni evolutive delle fattispecie penali esistenti e ad una produzione di nuove specifiche norme incriminatrici, ma via via anche ad una valorizzazione dei principi e diritti fondamentali da salvaguardare in questo peculiare campo, con l'affermazione, ad esempio, fin dal 1997, da parte della Corte Suprema statunitense[5], del diritto alla piena libertà di espressione ed informazione in Internet; quindi, del diritto alla riservatezza e sicurezza dei propri dati e "spazi" informatici, quale diritto fondamentale ricon-

[5] Cfr. la famosa sentenza nel caso *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997), con cui è stato annullato il *Communications Decency Act* (CDA), per violazione del Primo Emendamento che garantisce la libertà di espressione (*freedom of speech*).

ducibile ai diritti della personalità, sia da parte della Corte europea dei diritti dell'uomo, che lo ha desunto dal diritto alla vita privata e familiare di cui all'art. 8 della Convenzione europea[6], sia da parte di molte Corti costituzionali, in specie di quella tedesca[7], che l'ha incluso fra i «diritti generali della personalità» di cui all'art. 2 del *Grundgesetz*, riferibili alla stessa «dignità della persona umana» (*Menschenwürde*) di cui al suo art. 1.

Estremamente significativo è poi l'inserimento, nella "Carta dei diritti fondamentali" dell'Unione europea, approvata a Nizza nel 2000, di un inedito art. 8, che menziona in modo esplicito il diritto alla "Protezione dei dati di carattere personale", subito dopo quello alla vita privata e familiare, riconosciuto nell'art. 7 in termini simili a quelli con cui era già accolto nella Convenzione europea del 1950. Ed un riferimento assai importante, sul piano delle nuove fonti di produzione del diritto, è costituito oggi dall'art. 16 del Trattato sul funzionamento dell'Unione europea, che nel proclamare il «diritto alla protezione dei dati di carattere personale» in perfetta sintonia con il contenuto del menzionato art. 8 della Carta dei diritti fondamentali, prevede un esplicito potere normativo del Parlamento europeo e del Consiglio di regolarne, tramite procedura legislativa ordinaria, l'esercizio effettivo e di stabilire la disciplina della loro "circolazione" (par. 2), nel pieno rispetto, dunque, delle esaminate esigenze di democraticità delle fonti e di pieno coinvolgimento anche dei Parlamenti nazionali. Su tale base giuridica, l'Unione europea ha emanato – nelle more della pubblicazione del presente volume, essendo all'epoca del Convegno in fase avanzata di ap-

[6] Per una rassegna sistematica al riguardo si veda cfr. *Handbook on European data protection Law* (2014) consultabile al sito del Consiglio d'Europa (*www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf*) che si fonda, oltre che sull'art. 8 della Convenzione citata, sull'apposita *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale* (n. 108) adottata a Strasburgo il 28 gennaio 1981, e successivi protocolli addizionali.

Da menzionare anche la sentenza della Corte di Strasburgo 18 dicembre 2012, *Ahmet Yildirim c. Turquie*, nella quale è stata ravvisata la violazione dell'art. 10 della Convenzione nell'oscuramento di un sito internet, in quanto ingerenza non giustificata restrittiva del diritto alla libertà d'espressione in rete.

[7] Bundesverfassungsgericht, 27 febbraio 2008, 1 BvR 370/07, in *www.bundesverfassungsgericht.de*.

provazione – un regolamento di carattere generale per la protezione delle persone fisiche in relazione al trattamento dei dati personali[8], che sostituisce la direttiva 95/46/CE, ed una nuova più specifica direttiva, relativa 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[9].

Tali nuove disposizioni si collegano strettamente agli importanti sviluppi della giurisprudenza della Corte di giustizia dell'Unione europea, che negli ultimi anni ha avuto modo di fissare importanti principi di garanzia dei diritti fondamentali nel campo del trattamento dei dati personali, operando chiari bilanciamenti a loro favore. Mi riferisco in particolare a due sentenze della Grande Sezione del 2014, con cui rispettivamente è stata annullata la c.d. direttiva Frattini sulla *data retention* e poco dopo espressamente affermato il "diritto all'oblio" delle persone interessate ad un determinato trattamento di dati che le riguardino. La direttiva annullata imponeva, infatti, agli *Internet Service Providers* uno sproporzionato obbligo di raccolta ed archiviazione "preventiva" dei dati di traffico – da considerare ad ogni effetto quali dati personali – rispetto alle concrete esigenze delle indagini penali su gravi specifici reati, che pur potrebbero giustificarlo, ma soltanto con il presidio di concrete garanzie[10]. Mentre nel famoso caso Google, la Corte di giustizia ha solennemente dichiarato il "diritto all'oblio" rispetto a fatti obsoleti, la cui diffusione non sia supportata da un valido motivo d'interesse

[8] Si tratta del Regolamento (UE) 2016/679 del 27 aprile 2016 che stabilisce norme generali per la protezione delle persone fisiche in relazione al trattamento dei dati personali e per la libera circolazione dei dati personali nell'Unione.

[9] Si tratta della Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, parimenti del 27 aprile 2016, relativa «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» che abroga e sostituisce la decisione quadro 2008/977/GAI del Consiglio.

[10] Corte di giustizia dell'Unione europea (Grande Sezione), 8 aprile 2014, C-293/12 e C-594/12, *DigitalRights Ireland Ltd c. Minister for Communications*, etc., in *http://curia.eu*. Per un commento, anche alla luce della giurisprudenza costituzionale di diverse corti nazionali, si veda R. FLOR, *La Corte di giustizia considera la Direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Rivista trimestrale diritto penale contemporaneo*, n. 2, 2014, 178 ss.

collettivo o di terzi, con corrispondente obbligo del responsabile del motore di ricerca di escluderne l'indicizzazione in rete[11]. Si è così tracciata un'importante linea di bilanciamento fra i diritti fondamentali della persona, da un lato, e le libertà d'informazione, di comunicazione e di impresa nel *Cyberspace*, dall'altro, non potendo queste esercitarsi a discapito dei primi, con tutti i precipitati, anche a livello penalistico, delle responsabilità che possono scaturire dalle relative violazioni, fermo il criterio guida della "proporzione" da applicare nella valutazione e decisione dei casi concreti.

6. Da questi pur veloci riferimenti si conferma in modo paradigmatico l'incisività ed importanza degli strumenti giuridici, che il recente sviluppo 'multilivello' delle fonti mette a disposizione del giurista "moderno". Si tratta di valorizzarli e calarli sapientemente nella produzione ed elaborazione del diritto vivente, facendo sì che esso sia costantemente adeguato alle "sfide" cui deve far fronte, nel sempre rinnovato contesto globale, abbandonando l'idea – di matrice giusnaturalistica – che vi siano principi immutabili ed universali pre-confezionati, aventi un aprioristico valore assoluto, laddove occorre invece, con attenzione e sistematicità, riconoscerli, ricostruirli, dimensionarli nel bilanciamento reciproco, muovendo dalla pluralità di Carte dei diritti, di convenzioni e giurisdizioni internazionali, nonché di tradizioni costituzionali, da cui vanno oculatamente e pazientemente ricavati, per essere adattati alle nuove realtà emergenti, secondo il menzionato canone di proporzione, che è necessario guidi e controlli l'operato concreto dei giudici e degli stessi legislatori.

E sia consentita, al riguardo, una notazione critica meramente esemplificativa sull'operato del nostro legislatore, che per rafforzare gli strumenti penali di contrasto al terrorismo, con il decreto legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, nell'ambito di ben più incisivi interventi novellistici in gran parte richiesti dagli strumenti sovranazionali, ha anche aggiunto

[11] Corte di giustizia dell'Unione europea (Grande Sezione), 13 maggio 2014, C-131/12, Google Spain, Google Inc. c. AEPD e Mario Costeja Gonzalez, in *http://curia.eu*.

una circostanza aggravante al delitto di «addestramento ad attività con finalità di terrorismo anche internazionale» di cui all'art. 270-*quinquies* del codice penale, consistente nel fatto di «chi addestra o istruisce» (…) «attraverso strumenti informatici o telematici». Non si comprende la *ratio* di tale aggravamento di pena, rispetto al contenuto della fattispecie base ed al contesto sistematico degli altri delitti di terrorismo, non essendo evidente alcun elemento specifico di maggior pericolosità od offensività. Piuttosto l'impressione è di una generica "diffidenza", se non estraneità, nei confronti della tecnologia informatica e telematica, vista come minaccia globale cui viene data una risposta non congrua, che non distingue fra singoli strumenti, eventualmente limitabili ovvero utilizzabili anche positivamente, proprio per contrastare il terrorismo, ad esempio raccogliendo, incrociando ed analizzando prove nel *Cyberspace*. Questo è dunque il punto: se c'è un'approssimativa considerazione del dato tecnico, se c'è la sottovalutazione del contenuto specifico delle attività da contrastare o dei dati da ricercare nello spazio cibernetico, e degli strumenti più efficaci da utilizzare, è chiaro il rischio d'interventi indiscriminati, che non riescono a discernere fra diversi livelli e modi dell'intervento preventivo o repressivo, violando il principio di ragionevolezza, prima ancora che di proporzione.

Il nostro sforzo dovrebbe dunque essere questo: i principi li abbiamo, gli strumenti sovranazionali sono validi, ma occorre una competenza anche tecnica, oltre che giuridica, che consenta di calarli nella realtà concreta del *Cyberspace*, adeguandoli perennemente all'evoluzione globale per tracciare il confine fra quanto è accettabile o meno, al fine di perseguire obiettivi determinati, rifuggendo da posizioni generalizzanti di totale rifiuto o di acritica adesione a queste nuove formulazioni e metodologie, specie se comportino forti anticipazioni di tutela, che non sono di per sé giustificabili per la sola necessità del contrasto al terrorismo o ad altre gravi forme di criminalità, ma che neppure sono da escludere *a priori*, se proporzionate al sacrificio dei diritti da comprimere in relazione agli strumenti disponibili ed agli obiettivi da raggiungere[12].

[12] Per una paradigmatica vicenda in cui è di recente emersa la necessità di tracciare un confine fra tutela della *privacy* e moderni sistemi d'indagine, che vanno ben oltre le mere "intercettazioni ambientali", tramite l'utilizzo del c.d. "captatore elettronico", si

7. Sono dunque convinto che Roberto Flor ed Ivan Salvadori, cui dò finalmente la parola, forniranno con le loro articolate analisi chiare risposte alle questioni sul tappeto, dimostrando in concreto l'utilità dell'approccio metodologico sviluppato.

Il primo tratterà dei problemi relativi alla prevenzione e repressione del terrorismo in rete, con specifica attenzione al ruolo degli *Internet Service Providers* ed alla necessaria cooperazione, per garantire la sicurezza nel *Cyberspace* (la c.d. *Cybersecurity*), fra autorità pubbliche ed imprese private; il secondo si occuperà della più specifica questione della punibilità dei c.d. *dual-use software*, analizzandola, però, nel più ampio contesto dell'incriminazione degli atti preparatori di gravi reati che si possono commettere nel *Cyberspace* e tramite la tecnologia informatica, e così toccando profili ermeneutici, di diritto sovranazionale e di teoria del reato.

Si tratta di argomenti che, da un lato, richiedono adeguate conoscenze tecnico-informatiche, poiché solo su dette basi è possibile affrontare un'analisi corretta delle fattispecie vigenti e suggerire eventuali modifiche o nuove formulazioni; ma che, d'altro lato, devono misurarsi con i principi classici e tuttora basilari del diritto penale, che ne segnano i limiti in uno Stato democratico: quali in specie il principio di necessaria offensività del reato, previa individuazione dei beni giuridici di volta in volta meritevoli e bisognosi di protezione di fronte alle nuove forme di criminalità da contrastare; di *extrema ratio* o sussidiarietà dell'intervento penale, rispetto ad altri strumenti alternativi di intervento che possano garantire analoga efficacia; di personalità della responsabilità penale e di colpevolezza, il cui rispetto è condizione di legittimità del ricorso alla pena.

Aggiungo un'ultima notazione. L'importanza crescente del tema della criminalità informatica o, meglio, della criminalità nel *Cyberspace*, la sua articolazione in molteplici sottosettori, che vanno dai reati informatici in senso proprio del codice penale – quali frodi, falsi, dan-

---

veda Cass., sez. un., 1 luglio 2016 (28 aprile 2016), n. 26889/2016, Scurato, che si può leggere in *www.archiviopenale.it*. Nell'ampio dibattito sviluppatosi al riguardo, sia consentito rinviare a L. Picotti, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Archivio penale*, 2016, n. 2.

neggiamenti, accessi abusivi, intercettazioni – a quelli in senso ampio, soprattutto della legislazione speciale, in particolare in materia di trattamento di dati personali e di protezione dei diritti d'autore, fino alle nuove emergenze della pedopornografia e dell'adescamento di minori in rete, del cyberbullismo e degli abusi nei *social networks*, del *phishing*, del cyberterrorismo, del *cyberlaundring* con la connessa urgenza di sviluppare teoria e prassi nel campo, della *computer forensic* e, più in generale, delle prove elettroniche nelle indagini su qualsivoglia reato, con i correlati temi concernenti il ruolo e le responsabilità dei *Service Provider* nonché dei gestori di siti e di blog, ecc., ci hanno fatto sentire la necessità di creare uno strumento d'ausilio e, allo stesso tempo, di un *contact point* per gli operatori del diritto e la realtà economica e sociale interessata, in grado di raccogliere ed aggiornare fonti normative e giurisprudenziali, riferimenti bibliografici essenziali, materiali e contributi significativi od attuali, progetti di ricerca e buone prassi, interventi in dibattiti e convegni, iniziative di studio e di scambio che si sviluppano quotidianamente in materia.

L'idea è stata di creare l'"Osservatorio Cybercrime" (*https://www.cybercrime.dsg.univr.it*), quale sito dinamico nel *web*, in cui convogliare tali esperienze e conoscenze, per sviluppare una rete di rapporti ed adesioni – in ambito accademico, professionale, giudiziario, tecnico, aziendale, sociale, ecc. – che consenta di stimolare e far circolare nuovi contributi, segnalazioni, esperienze, non solo giuridiche o dottrinali, ma anche operative, applicative, progettuali, ecc., a livello nazionale e sovranazionale.

La convinzione è che spesso fenomeni gravi, quali ad es. la pedopornografia, di fatto sollecitino norme e tecniche d'intervento, che poi si possono estendere ed applicare anche ad altri fenomeni, anche più gravi, quali il terrorismo e la lotta al suo finanziamento, a sua volta strettamente connessa a quella al riciclaggio, con un travaso di esperienze, strumenti e regole, come sottolineava prima anche John Vervaele, da un settore ad un altro: per cui l'attenzione richiamata su uno, in cui si ha la percezione della punta di un *iceberg*, che sottende interventi punitivi od investigativi anche *extra ordinem*, serve a valutare criticamente quell'esperienza ed eventualmente frenare la sua potenziale ca-

pacità espansiva, ovvero a trasformarla in un modello per uno sviluppo ulteriore, a seconda che sia o meno accettabile od auspicabile.

Per questo – e concludo davvero quest'introduzione un po' troppo lunga ed appassionata, di cui mi scuso: ma sono argomenti che da tanti anni ci prendono – lo sforzo è di far circolare e trasmettere l'esperienza e l'impegno alle nuove generazioni di giuristi e di studiosi, perché non solo mantengano costantemente aggiornate le specifiche conoscenze e competenze nell'ambito del diritto penale dell'informatica (e non solo), ma soprattutto rendano sempre vivi ed attuali i principi di garanzia e di legittimità democratica che devono presiedervi, essendo questo l'apporto caratterizzante del nostro lavoro, che certamente Roberto ed Ivan sapranno interpretare nel modo migliore.

# CYBER-TERRORISMO E DIRITTO PENALE IN ITALIA[*]

*Roberto Flor*

SOMMARIO: *1. Introduzione. 2. Il fenomeno cyber-terrorismo. 3. Cyber-terrorismo e diritto penale in Italia. 3.1. Cyber-terrorismo e criminalità informatica. 3.2. Cyber-terrorismo e legislazione anti-terrorismo. 4. Riflessioni conclusive.*

## *1. Introduzione*

Il fenomeno terroristico ha subito un mutamento sostanziale, in specie negli ultimi anni, a partire dagli attentati di New York (2001), Madrid (2004) e Londra (2005).

Questa trasformazione è dovuta, da un lato, alla progressiva adozione di strategie tipiche dei comandi militari – come nei casi degli attacchi alla redazione di Charlie Hebdo (2015) o di quelli perpetrati dall'ISIS (Islamic State of Iraq and Sirya) dal 2014, nonché di quelli legati agli ultimi tragici avvenimenti di Parigi, Berlino ed Istanbul – dall'altro lato al crescente utilizzo delle nuove tecnologie, sia nelle fasi organizzative e preparatorie, sia in quelle esecutive (e successive) all'attentato, in parte anche tramite lo sfruttamento di informazioni e notizie pubblicate su testate giornalistiche *online*, *social media* e *social networks*[1].

[*] Il presente contributo costituisce uno dei risultati della ricerca "Nuove tecnologie e lotta al (cyber)terrorismo ed al discorso d'odio in prospettiva europea", Progetto finanziato nell'ambito del *Programma di Ricerca di Base 2015* promosso dall'Università di Verona, di cui è responsabile scientifico Roberto Flor.

[1] Ne sono un esempio emblematico la vicenda Centcom, in relazione alla quale si è parlato di Cyberjihad, e le attività di indagine in relazione agli attentati parigini per rintracciare i componenti delle cellule terroristiche. Si fa riferimento all'attacco informatico del 12 gennaio 2015 attuato dall'ISIS contro la banca-dati e l'account twitter @Centcom – U.S. Central Command – del Comando statunitense che controlla le operazioni contro lo Stato islamico in Siria ed Iraq. Non a caso all'indomani degli attacchi nella capitale

Internet consente non solo la delocalizzazione delle risorse, anche grazie alla nuova dimensione del *cloud*[2] e della "struttura" del *web*, ma altresì la detemporalizzazione delle attività, che possono essere pianificate e svolte attraverso operazioni automatizzate programmate dall'utente, che fanno venire meno l'esigenza di un "collegamento" o "contatto" fisico fra persona e sistema informatico, nonché la deterritorializzazione dell'utente, il quale può svolgere un'operazione complessa essendo "presente virtualmente" in più "luoghi-spazi informatici" anche nello stesso momento e attraverso più macchine-sistemi.

La rete conosciuta dalla quasi totalità degli utenti, inoltre, costituisce solamente la punta di un grande *iceberg*. La parte "sommersa" e più consistente è il c.d. *deep web*, ossia uno spazio colmo di risorse informative del *World Wide Web* non segnalate o indicizzate dai normali motori di ricerca, a cui è possibile accedere solo tramite specifici *softwares* o *browsers* e all'interno del quale è possibile svolgere ogni tipo di attività – legale o illegale – grazie alle potenzialità offerte dalle diverse forme di anonimato utilizzabili, anche tramite tecniche di dissimulazione dell'*ip address*[3] che possono far apparire provenienze "territoriali" false o errate[4].

---

francese il collettivo di "hacktivisti" più celebre del web (Anonymous) aveva diffuso un video in diverse lingue in cui minacciava l'Isis, preannunciando una caccia all'uomo online e di oscurare i profili digitali dei membri – o dei simpatizzanti – dello Stato Islamico. Oppure si pensi alle recenti operazioni contro le reti ISIS gestite e condotte dall'Us Cyber Command, che affianca l'Nsa (vedi D.E. SANGER, *U.S. Cyberattacks Target ISIS in a New Line of Combat*, in *The NYT*, 24 aprile 2016).

[2] La nozione di *cloud computing* allude ad un insieme di tecnologie che permettono di memorizzare, archiviare e/o elaborare dati grazie all'utilizzo di risorse *hardware/ software* delocalizzate in rete. Cfr., per una spiegazione tecnica, B. FURHT, A. ESCALANTE, *Handbook of Cloud Computing*, Boca Raton (FL), 2010. Con riferimento alle possibili problematiche sul piano giuridico, anche con riferimento alla tutela dei dati e delle informazioni, vedi Y. POULLET, J.M. VAN GYSEGHEM, J. GÉRARD, C. GAYREL, J.P. MOINY, *Cloud computing and its implications on data protection*, Discussion paper, Council of Europe, Strasbourg, 2010; L. BUONO, *The Global Challenge of Cloud Computing and EU Law*, in *Eucrim*, 3/2010, 117 ss.; J. SPOENLE, *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, Discussion paper, Council of Europe, Strasbourg, 2010.

[3] Esistono molteplici modi per nascondere o rendere non tracciabile l'*ip address* dell'attaccante reale. Cfr. EC Council, *Ethical Hacking and Countermeasures: Attack*

In questo contesto, già di per sé complesso, si innesta il c.d. "cyber-terrorismo".

La minaccia del "cyber-terrorismo" e dell'uso di Internet per propositi terroristici è particolarmente allarmante, proprio per la forte dipendenza dell'attuale assetto sociale, economico e politico dalla informatizzazione e dalla rete globale.

Tale fenomeno criminoso, anche se non è ben definito, è certamente rappresentativo del ruolo che l'evoluzione tecnologica svolge nel pianificare e/o nell'eseguire attacchi terroristici. Inoltre gli stessi obiettivi degli attacchi possono essere i sistemi informatici e le banche dati sensibili degli Stati o delle istituzioni europee, ovvero i dati e le informazioni ivi archiviati o, ancora, i sistemi di comunicazione basati su infrastrutture logiche e reti telematiche.

Le tecnologie dell'informazione e della comunicazione, al contempo, se regolate giuridicamente, possono svolgere una funzione essenziale nella prevenzione, nel contrasto e nell'accertamento degli illeciti. Si pensi, ad esempio, all'oscuramento od al blocco di siti Internet, all'accesso segreto a sistemi informatici, al monitoraggio della rete o alla conservazione dei dati di traffico telematico per finalità investigative.

Recentemente nel contrasto al terrorismo si è assistito, in particolare con il d.l. n. 7 del 2015 convertito con la l. n. 43 del 2015 e la l. n. 153

---

*Phases*, New York, 2010, 3-14; S. GHOSH, E. TURRINI, *Cybercrimes: A Multidisciplinary Analysis*, Berlin-Heidelberg, 2010, 56 ss. Per una indagine sul piano tecnico-informatico vedi C. ELISAN, *Malware, Rootkits & Botnets A Beginner's Guide Malware*, New York, 2013.

[4] Per alcune informazioni sul web sommerso, accessibili all'opinione pubblica italiana, vedi, fra le più recenti indagini giornalistiche, quelle di Focus (2014) *http://www.focus.it/tecnologia/innovazione/cinque-cose-da-sapere-sul-deep-web*; del Corriere della Sera (2012) *http://www.corriere.it/inchieste/droga-armi-minori-killer-viaggio-deep-web-zona-web-senza-regole-morale-dove-tutto-possibile/44ed8fce-8935-11e1-a8e9-f84c50c7f614.shtml*; del Fatto Quotidiano (2015) *http://www.ilfattoquotidiano.it/2015/04/10/deep-web-vende-rete-invisibile-dalle-carte-credito-badge-polizia/1577620/*. Vedi anche C. FREDIANI, *Deep Web - La rete oltre Google - Personaggi, storie e luoghi dell'internet profonda*, Genova, 2014. Con riferimento all'uso del deep web e, in particolare di Tor, nelle investigazioni informatiche cfr. T.G. SHIPLEY, A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, 2014, in specie 219 ss.

del 2016, ad un tentativo di rafforzamento delle norme interne, sia sul piano del diritto penale sostanziale che su quello della cooperazione fra settore pubblico (*law enforcement*) e settore privato (soprattutto Internet Service Provider, ossia i fornitori di servizi nella società dell'informazione)[5].

[5] Sul piano del diritto penale sostanziale possono essere individuate almeno tre aree di intervento: 1. è stato inasprito il trattamento sanzionatorio delle condotte soggettivamente mirate al compimento di atti terroristici; 2. è stata anticipata la tutela in materia di esplosivi incriminando fatti concernenti i c.d. precursori; 3. è stata rafforzata l'efficacia delle misure di prevenzione, estese anche ai cosiddetti foreign fighters attraverso nuove misure punitive per le relative violazioni. Con la novella del 2016, inoltre, il legislatore è intervenuto in materia di finanziamento di condotte con finalità di terrorismo (art. 270 quinquies.1 c.p.); Sottrazione di beni o denaro sottoposti a sequestro (art. 270 quinquies.2 c.p.); Atti di terrorismo nucleare (art. 280 ter c.p.). Con riguardo al sistema italiano, sulla l. n. 155 del 2005 vedi fra i primi commenti A. VALSECCHI, *Il problema della definizione di terrorismo*, in *Riv. it. dir. proc. pen.*, 2005, 1127 e ss.; A. VALSECCHI, *La definizione di terrorismo dopo l'introduzione del nuovo art. 270 sexies c.p.*, in *Riv. it. dir. proc. pen.*, 2006, 1103 e ss. Per una prospettiva più ampia, europea ed internazionale, nonché per approfondite riflessioni sulla lotta al terrorismo, sistema penale e tutela dei diritti fondamentali, basti il rinvio a F. VIGANÒ, *Lucha contra el terrorismo y protección de los derechos fundamentales*, in L.A. ZAPATERO, *Piratas, mercenarios, soldados, jueces y policías: nuevos desafíos del Derecho penal europeo e internacional*, Cuenca, 2010, 77 e ss. Vedi anche F. VIGANÒ, *Terrorismo, guerra e sistema penale*, in *Riv. it. dir. proc. pen.*, 2006, 648 e ss.; nonché F. VIGANÒ, *La nozione di "terrorismo" ai sensi del diritto penale*, in F. SALERNO (cur.), *Sanzioni "individuali" del Consiglio di Sicurezza e garanzie processuali fondamentali*, Padova, 2010, 193 e ss. Con riferimento al dibattito relativo al "diritto penale del nemico", cfr. in questa sede M. DONINI, *Diritto penale di lotta vs. diritto penale del nemico*, in R.E. KOSTORIS, R. ORLANDI (cur.), *Contrasto al terrorismo interno e internazionale*, Torino, 2006, 19-73. Sul contrasto al terrorismo vedi, nella più recente letteratura internazionale e senza pretesa di esaustività, anche in prospettiva europea e comparata, J.A.E. VERVAELE, *Counterterrorism: net widening and function creep in criminal justice*, in *Dir. pen. XXI sec.*, 2015, 205 ss.; C.C. MURPHY, *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law*, Oxford, 2012; A. MASFERRER, C. WALKER (eds.), *Counter-Terrorism, Human Rights and the Rule of Law*, Cheltenham, 2013; K. ROACH (ed.), *Comparative Counter-Terrorism Law*, New York, 2015; H. DUFFY, *The 'War on Terror' and the Framework of International Law*, II ed., Cambridge, 2015. Cfr. anche F. GALLI, *The Law on Terrorism: The UK, France and Italy compared*, Brussels, 2015. Sul finanziamento al terrorismo, anche tenendo conto del ruolo di Internet e delle nuove tecnologie, vedi U. SIEBER, B. VOGEL, *Terrorismusfinanzierung. Prävention im Span-*

Sul piano investigativo invece, e più in specifico su quello dei mezzi di ricerca della prova, non si rinvengono novità di rilievo, neppure dopo la storica sentenza della Corte di giustizia in materia di *data retention*[6].

Il presente lavoro si concentrerà sull'analisi critica delle recenti disposizioni in materia di contrasto e prevenzione al terrorismo con specifico riferimento al "contesto tecnologico".

Appare però opportuno, preliminarmente, tentare di definire il fenomeno terroristico nell'era delle tecnologie della comunicazione e dell'informazione.

## *2. Il fenomeno cyber-terrorismo*

Il cyber-terrorismo è da tenere anzitutto distinto dalla c.d. *cyber-war*[7].

---

*nungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht*, Berlin, 2015. Si rinvia, più in generale, a M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale al limite*, nonché M. DONINI, *Terrorismo e ruolo della giurisdizione. Dal codice delle indagini preliminari a quello postdibattimentale*, entrambi in *QG (speciali)*, 2016, rispettivamente 99 ss., 113 ss.; cfr. inoltre F. FASANI, *Terrorismo islamico e diritto penale*, Milano, 2016; A. CAVALIERE, *Considerazioni critiche intorno al d.l. antiterrorismo n. 7 del 18 febbraio 2015*, in *Dir. pen. cont. trim.*, 2/2015, 226 ss.; R.E. KOSTORIS, F. VIGANÒ (cur.), *Il nuovo pacchetto anti terrorismo*, Torino, 2015; V. MASARONE, *Politica criminale e diritto penale nel contrasto al terrorismo internazionale*, Napoli, 2013. Sulla cooperazione fra settore pubblico e privato nella lotta al terrorismo nell'era tecnologica vedi R. FLOR, *Il contrasto al terrorismo nell'era delle nuove tecnologie e i meccanismi di cooperazione fra settore pubblico e settore privato*, in *Scritti in onore di Stortoni*, Bologna, 2016, 513 ss.

[6] Vedi Corte di giustizia dell'Unione europea, 8 aprile 2014 (C-293/12, C-594/12). Cfr. R. FLOR, *La giustizia penale nella rete? Tutela della riservatezza versus interesse all'accertamento e alla prevenzione dei reati nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in R. FLOR, D. FALCINELLI, S. MARCOLINI (cur.), *La giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di Internet*, Milano, 2015, 153 e ss.

[7] R.A. CLARKE, R. KNAKE, *Cyber War: The Next Threat to National Security and What to Do About It*, New York, 2010; M.C. LIBICKI, *Cyberdeterrence and Cyberwar*, Santa Monica (CA), 2009; P. SHAKARIAN, J. SHAKARIAN, A. RUEF, *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, Waltham, 2013; P.W. SINGER, A. FRIEDMAN, *Cybersecurity and cyberwar: what everyone needs to know*, Oxford-New York,

In primo luogo, sul piano fenomenico, pare opportuno adottare, fra le molteplici definizioni[8], una ampia concezione di terrorismo, che comprenda l'uso illegale della forza o della violenza, o la minaccia di tale uso, connotati da fini politici, ideologici o religiosi, contro persone o beni, per intimidire o coartare un governo o la popolazione civile, anche sul piano "psicologico" (quale potrebbe essere l'incremento della paura o della percezione della paura)[9].

Essa può ricomprendere anche la definizione legale italiana della "finalità terroristica", ex art. 270 sexies c.p., per cui sono considerate con finalità di terrorismo le condotte che, per la loro natura o il loro "contesto", possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono realizzate allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale.

La formulazione della Convenzione del 1999 [Convenzione ONU contro il finanziamento del terrorismo], resa esecutiva con la l. n. 7 del 2003,

---

2014; M. CHAPPLE, D. SEIDL, *Cyberwarfare: Information Operations in a Connected World*, Burlington, 2015. Vedi anche N. ABOUZAKHAR (ed.), *Proceedings of the 14th European Conference on Cyber Warfare and Security*, Reading, 2015; M.N. SIROHI, *Cyber Terrorism and Information Warfare*, Dehli, 2015; T.M. CHEN, L. JARVIS, S. MACDONALD (eds.), *Cyberterrorism: Understanding, Assessment, and Response*, New York, 2014. Cfr. altresì CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM (ed.), *Responses to Cyber Terrorism*, Amsterdam, 2008.

[8] Si pensi che una risalente ricerca aveva evidenziato più di 100 diverse definizioni di terrorismo. Vedi AA.VV., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*, New Brunswick (NJ), 1988, 5 e ss.

[9] Tale definizione è in parte accolta anche da U. SIEBER, P. BRUNST, *Cyberterrorism: the use of the Internet for terrorist purposes*, Council of Europe Pub., Strasburgo, 2007, 14 e ss. Sulla definizione di terrorismo vedi, inoltre, B. HOFFMAN, *Defining Terrorism*, in R. HOWARD, R. SAWYER (eds.), *Terrorism and Counterterrorism: Understanding the New Security Environment*, Guilford (CT), 2003, 22 e ss.

> ha una portata così ampia da assumere il valore di una definizione generale, applicabile sia in tempo di pace che in tempo di guerra e comprensiva di qualsiasi condotta diretta contro la vita o l'incolumità di civili o, in contesti bellici, contro "ogni altra persona che non prenda parte attiva alle ostilità in una situazione di conflitto armato", al fine di diffondere il terrore fra la popolazione o di costringere uno stato o un'organizzazione internazionale a compiere o a omettere un atto […] con l'ulteriore requisito della motivazione politica, religiosa o ideologica, conformemente a una norma consuetudinaria internazionale accolta in varie risoluzioni dell'Assemblea Generale e del Consiglio di Sicurezza dell'ONU, nonché dalla Convenzione del 1997 contro gli attentati terroristici commessi con l'uso di esplosivi[10].

La definizione formulata dal Consiglio dell'Unione europea con la decisione quadro 2002/475/GAI «sulla lotta contro il terrorismo», non si discosta molto da quella della Convenzione ONU, se non per due eccezioni: in primo luogo, la decisione quadro non può trovare applicazione (in base all'undicesimo considerando) a fatti commessi in contesti bellici; in secondo luogo, la definizione della decisione quadro, include fra le possibili 'finalità terroristiche', accanto alla diffusione del terrore e la coazione della volontà di un paese o di un'organizzazione internazionale, anche il fine di «destabilizzare gravemente o distruggere le strutture politiche fondamentali, costituzionali, economiche o sociali di un Paese o di un'organizzazione internazionale»[11].

Sono note le criticità legate alla definizione della «finalità di terrorismo», ex art. 270 sexies c.p., adottata dal nostro legislatore[12]. Essa ripro-

[10] Vedi Cass., sez. I pen., 11 ottobre 2006, n. 1072 (Bouyahia), in Ced 235289; C. Ass. Milano, 9 maggio 2005, Bouyahia, in *Riv. it. dir. e proc. pen*., 2005, 821 e ss.

[11] A. VALSECCHI, *I requisiti oggettivi della condotta terroristica ai sensi dell'art. 270 sexies c.p. (prendendo spunto da un'azione dimostrativa dell'animal liberation front)*, in *Dir. pen. contemporaneo*, 21 febbraio 2013.

[12] Recentemente ricordate da A. CAVALIERE, *Considerazioni critiche*, cit., 226 ss. In questa sede basti il rinvio a T. PADOVANI, *Commento all'art. 15, d.l. 27.7.2005, n. 144, conv. con modif. in l. 31.7.2005, n. 155*, in *Leg. pen.*, 2005, 557 ss.; T. PADOVANI, *Un intervento normativo scoordinato che investe anche i delitti contro lo Stato*, in *Guida dir.*, 2006, 14, 23 ss.; M. PELISSERO, *Terrorismo internazionale e diritto penale*, in *St. iuris*, 2005, 1286 ss.; A. VALSECCHI, *Misure urgenti per il contrasto del terrorismo internazionale. Brevi osservazioni di diritto penale sostanziale*, in *Dir. pen. proc.*, 2005, 1222 ss.; E. ROSI, *Le modifiche al diritto penale sostanziale*, in E. ROSI, S. SCO-

duce solo la prima parte dell'art. 1 della decisione quadro 2002/475/GAI (che dovrebbe essere sostituita dalla [proposta di] direttiva del 2 dicembre 2015)[13], tralasciando l'elenco degli "atti intenzionali" che, per il legislatore dell'Unione europea, avrebbero dovuto essere i soli a meritare la qualifica di "reati terroristici" quando, «per la loro natura o contesto possono arrecare grave danno a un paese o a un'organizzazione internazionale» e siano commessi al fine di

> intimidire gravemente la popolazione, costringere indebitamente i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto, o destabilizzare gravemente o distruggere le strutture politiche fondamentali, costituzionali, economiche o sociali di un paese o un'organizzazione internazionale.

D'altra parte l'assetto attuale della lotta al terrorismo a livello internazionale evoca pericolose commistioni tra guerra e diritto, ovvero, correlativamente, fra attacco armato, crimine internazionale e reato "comune"[14].

---

PELLITI (cur.), *Terrorismo internazionale. Modifiche al sistema penale e nuovi strumenti di prevenzione*, Milano, 2006, 62 ss.; M. MANTOVANI, *Le condotte con finalità di terrorismo*, in R.E. KOSTORIS, R. ORLANDI (cur.), *Contrasto al terrorismo interno ed internazionale*, Torino, 2007, 79 e ss.; F. VIGANÒ, *La nozione di "terrorismo" ai sensi del diritto penale*, in F. SALERNO (cur.), *Sanzioni "individuali" del Consiglio di Sicurezza e garanzie processuali fondamentali*, Padova, 2010, 193 ss. Cfr. anche A. BERARDI (cur.), *Il diritto e il terrore: alle radici teoriche della "finalità di terrorismo"*, Padova, 2008; R. BARTOLI, *Lotta al terrorismo internazionale. Tra diritto penale del nemico jus in bello del criminale e annientamento del nemico assoluto*, Torino, 2008. Vedi anche R. BARBERINI, *Terrorismo e forze armate: si è consolidato un equivoco*, in *Cass. pen.*, 2010, 3415 e ss.

[13] Proposta di direttiva del Parlamento europeo e del Consiglio sulla lotta contro il terrorismo e che sostituisce la decisione quadro del Consiglio 2002/475/GAI sulla lotta contro il terrorismo [COM(2015) 625 final].

[14] Fletcher ha prospettato una terza soluzione, parlando di «super-reato», che porta con sé le caratteristiche sia del diritto che della guerra. Vedi G.P. FLETCHER, *I fondamenti filosofico-giuridici della repressione del terrorismo*, in M. DONINI, M. PAPA (cur.), *Diritto penale del nemico: un dibattito internazionale*, Milano, 2007, 371. Vedi anche G.P. FLETCHER, *The Indefinable Concept of Terrorism*, in *J. Int'l Crim. Just.*, 2006, 894-911. Proprio l'incertezza sulla natura del fenomeno ha reso impossibile, ad oggi, addivenire ad una definizione giuridica condivisa a livello globale. Ne è una pro-

Le difficoltà appena rilevate non si attenuano certo nella ricerca di una definizione, anzitutto fenomenica, di cyber-terrorismo.

A tal fine è necessario distinguere almeno tre elementi o componenti caratterizzanti[15]:

1) gli attacchi che vengono realizzati tramite la rete telematica e le tecnologie, che possono cagionare il danneggiamento o l'alterazione del funzionamento di sistemi informatici "sensibili" o di sistemi di comunicazione, oppure delle infrastrutture dello Stato o degli enti pubblici essenziali per la stessa vita umana, ovvero il danneggiamento o la perdita di dati, anche "segreti" o "sensibili", ivi archiviati o trattati;
2) la diffusione di contenuti illegali attraverso la rete, volti non solo a fornire informazioni sulla preparazione di un attacco terroristico, ma anche a incitare, pubblicizzare, diffondere idee o opinioni, o a reclutare militanti, a raccogliere fondi per guerre ideologiche o per disseminare materiale di stampo razzista o xenofobico; in questo caso si tratta di attività che devono essere tenute distinte da quelle proprie dell'attivismo "pacifico", anche se sussistono alcuni elementi comuni come, ad esempio, la propaganda, il reclutamento, la ricerca o la raccolta di fondi e l'utilizzo delle nuove tecnologie a scopo diffusivo/comunicativo[16];

---

va la Convenzione globale sul terrorismo, la cui predisposizione è stata affidata nel 1996 ad uno speciale Comitato istituito dall'Assemblea Generale dell'ONU ma che ancora non ha visto la luce. Cfr. I. MARCHI, *Esigenze di sicurezza e diritti umani nel contrasto al terrorismo. Una prospettiva de iure condendo*, in *Dir. pen. XXI sec.*, 2015, 259 ss.; vedi anche cfr. R. BARBERINI, *Terrorismo e movimenti di liberazione nazionale: la Convenzione globale contro il terrorismo*, in A. DE GUTTRY (cur.), *Oltre la reazione. Complessità e limiti nella guerra al terrorismo internazionale dopo l'11 settembre*, Pisa, 2003, 107 ss.

[15] Cfr. U. SIEBER, P. BRUNST, *Cyberterrorism*, cit., 14 ss.; B.J. KOOPS, *Megatrends and Grand Challenges of Cybercrime and Cyber-Terrorism Policy and Research*, in B. AKHGAR, B. BREWSTER (eds.), *Combatting Cybercrime and Cyberterrorism. Challenges, Trends and Priorities*, New York, 2016, 3 ss.

[16] Cfr. R. REITAN, *Global activism*, New York, 2007, G. MEIKLE, *Media activism and the Internet*, London, 2002. Vedi anche L. JARVIS, S. MACDONALD, T.M. CHEN (eds.), *Terrorism Online: Politics, Law and Technology*, New York, 2015; G. WEIMANN, *Terrorism in Cyberspace: The Next Generation*, New York, 2015.

3) l'uso della rete e delle tecnologie quali strumenti di comunicazione fra terroristi o gruppi terroristici, che permette di fruire di sistemi di anonimato o di delocalizzazione del flusso di dati, nonché di frazionamento della tempistica della comunicazione, gestibile altresì attraverso procedimenti automatizzati e programmabili ex ante.

Una ulteriore classificazione fenomenica si basa sul "ruolo" della tecnologia e di Internet, distinguendo i casi in cui:

1) gli strumenti informatici, comprese le infrastrutture e la rete, costituiscono *solo uno* dei molteplici mezzi per la realizzazione di un attacco terroristico, nella fase preparatoria e/o esecutiva (si pensi al reperimento di informazioni online per la costruzione di un ordigno e per raccogliere dati sull'obiettivo fisico da colpire);
2) le tecnologie e la rete costituiscono gli *strumenti essenziali* o *indispensabili* per la preparazione o l'esecuzione di un attacco terroristico (si pensi alla diffusione di programmi malevoli al fine di interrompere servizi di pubblica utilità erogati tramite sistemi informatici), oppure costituiscono l'oggetto o l'*obiettivo* di tale attività, che potrebbero essere realizzate per forzare le misure di sicurezza al fine di accedere ai sistemi informatici, o di minare l'integrità, la confidenzialità o la segretezza dei *computer systems* e dei dati, ovvero per rendere i sistemi non operativi o inutilizzabili oppure, ancora, per alterare o falsificare dati e informazioni ivi contenuti o per rendere critiche infrastrutture "sensibili", generalmente connesse ad altre infrastrutture per l'erogazione di energia, acqua, trasporti, servizi di difesa nazionale, sanità pubblica, ordine pubblico[17].

[17] Cfr. U. SIEBER, P. BRUNST, *Cyberterrorism*, cit.; U. SIEBER, *Instruments of International Law: against Terrorist Use of the Internet*, in M. WADE, A. MALJEVIC (Hrsg.), *A War on Terror? The European Stance on a new Threat, Changing Laws and Human Rights Implications*, New York, 2010, 171-219.

## *3. Cyber-terrorismo e diritto penale in Italia*

### *3.1. Cyber-terrorismo e criminalità informatica*

Sul piano del diritto penale sostanziale, non si rinviene una fattispecie legale che tipizzi in senso unitario il fenomeno.

Dovendo dunque tentare di verificare l'astratta applicabilità delle disposizioni incriminatrici vigenti nel nostro ordinamento, appare preliminarmente necessario osservare che il "cyber-terrorismo" è caratterizzato da alcune componenti fenomeniche comuni sia alla criminalità informatica che al terrorismo "tradizionale".

Secondo una nota studiosa si dovrebbe far riferimento più propriamente ad una «convergenza fra cyberspazio e terrorismo», che dovrebbe coprire anche le c.d. *politically motivated hacking operations* realizzate per causare gravi danni alle istituzioni, all'economia ed alla vita ed all'integrità fisica[18].

Il disvalore del fenomeno sembra comunque essere connotato, da un lato, dall'atteggiamento psicologico – di natura politica o ideologica o culturale o religiosa o, in ogni modo, valoriale – e nemicale, che può assumere la qualifica di una finalità determinata.

Dall'altro lato, la direzione offensiva del "fatto" sembra avere come obiettivo la società civile incolpevole o comunque estranea al "conflitto"[19].

---

[18] Vedi D.E. DENNING, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, in J. ARQUILLA, D. RONFELDT (eds.), *Networks and netwars. The future of terror, crime and militancy*, Santa Monica, 2001, 239-288, in specie 241. Il termine *cyberterrorism* è stato coniato da B. COLLIN, *The Future of Cyberterrorism*, in *Crime and Justice International*, March 1997, 15-18, in cui descrive diversi scenari di ipotetici attacchi realizzabili attraverso le nuove tecnologie e la rete.

[19] Le componenti strutturali sinora descritte assumono diversa rilevanza in contesti in tempo di guerra e in tempo di pace. Nei primi, il conflitto armato contribuisce al deficit di autonomia dell'elemento legato all'atteggiamento soggettivo-psicologico ed assume invece maggiore importanza l'estraneità o la terzietà rispetto alle ostilità. Nei secondi, viceversa, il ruolo di protagonista è proprio dell'atteggiamento soggettivo-psicologico, inteso sia come scopo che come movente. Cfr. ampiamente, anche per un inquadramento dogmatico che valorizzi i confini fra diritto e guerra, S. HERBERT, *Grenzen des Strafrechts bei der Terrorismusgesetzgebung. Ein Rechtsvergleich zwischen*

La combinazione di questi "fattori", ossia la "convergenza" sopra citata, influenzerebbe le scelte di politica criminale, di sicurezza interna e di politica estera[20].

In Europa, con l'entrata in vigore del Trattato di Lisbona sia la "criminalità informatica" che il "terrorismo" sono stati inseriti nell'art. 83, par. 1, TFUE fra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione europea ha competenza penale.

In tali ambiti vi sono già concrete iniziative, in particolare la direttiva 2013/40/UE del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione, che sostituisce la decisione quadro 2005/222/GAI, e la proposta di direttiva del 2 dicembre 2015 relativa alla lotta al terrorismo[21]. Quest'ultima esprime, almeno in parte, quella «convergenza fra cyberspazio e terrorismo», nonché la consapevolezza che i gruppi terroristici hanno mostrato di saper utilizzare competenze nell'uso di Internet e delle nuove tecnologie per propaganda, reclutamento, condivisione di conoscenze, pianificazione e coordinamento delle operazioni.

Internet è diventato, in effetti, il canale principale per diffondere pubbliche minacce, glorificare atti terroristici atroci e rivendicare la responsabilità degli attentati. Per tali motivi il legislatore europeo ha evidenziato che: 1. le disposizioni di cui all'art. 5 della proposta di direttiva (Pubblica provocazione a commettere reati di terrorismo) inten-

---

*Deutschland und England*, Berlin, 2014; A. WILDFANG, *Terrorismus. Definition – Struktur – Dynamik*, Berlin, 2010; nella letteratura italiana vedi, in un'ottica di valorizzazione del ruolo dei diritti fondamentali nella definizione dello status di terrorista, a M. DONINI, *Lo status di terrorista: tra il nemico ed il criminale. I diritti fondamentali e la giurisdizione penale come garanzia contro, o come giustificazione per l'uso del diritto come arma*, in S. MOCCIA (cur.), *I diritti fondamentali della persona a prova dell'emergenza*, Napoli, 2009, 85 e ss.; F. PALAZZO, *Contrasto al terrorismo, diritto penale del nemico e principi fondamentali*, in *Verso un diritto penale del nemico?*, in *Questione Giustizia*, 2006, n. 4, 666 ss. Cfr. altresì, fra i molti contributi, M. DONINI, M. PAPA (a cura di), *Diritto penale del nemico. Un dibattito internazionale*, Milano, 2007; A. GAMBERINI, R. ORLANDI (cura di), *Delitto politico e diritto penale del nemico*, Bologna, 2007; M. DONINI, *Il diritto penale di fronte al «nemico»*, in *Cass. pen.*, 2006, 735 ss.; F. VIGANÒ, *Terrorismo, guerra e sistema penale*, in *Riv. it. dir. proc. pen.*, 2006, 648 ss.

[20] D.E. DENNING, *Activism*, cit., 288.

[21] COM(2015) 625 final - 2015/0281 (COD) del 2 dicembre 2015.

dono assicurare che sia perseguibile penalmente la diffusione in Internet di messaggi che incoraggiano la perpetrazione di reati terroristici; 2. le norme di cui all'art. 7 della proposta direttiva (Addestramento a fini terroristici) intendono contrastare anche la diffusione di istruzioni e manuali (online) ai fini dell'addestramento e della pianificazione di attentati e più specificamente la diffusione (attraverso Internet) di informazioni sulle risorse e i metodi terroristici, che funge in tal modo da "campo di addestramento virtuale".

Le modalità di commissione di un attacco terroristico, dunque, possono essere molteplici ed utilizzare sia mezzi più sofisticati (come, ad es., strutture logiche e connessioni complesse per realizzare attacchi informatici contro infrastrutture sensibili dello Stato), che strategie e modalità di esecuzione "tradizionali" (si pensi alla distruzione materiale dell'edificio in cui sono conservati *servers* e banche dati "sensibili" o "strategiche" o di "pubblica utilità").

La multiforme dimensione del cyber-terrorismo[22], quindi, rende potenzialmente applicabili al fenomeno le fattispecie penali in materia di reati informatici.

Sul piano sovranazionale è bene ricordare che la Convenzione di Budapest sul *Cybercrime* del 2001 (CC), attuata in Italia con la l. n. 48 del 2008[23], si applica non solo ai reati informatici in senso stretto da

[22] Cfr. ampiamente U. SIEBER, P. BRUNST, *Cyberterrorism and other use of Internet for terrorist purpose*, Strasburgo, 2007; U. SIEBER, *Instruments of International Law: against Terrorist Use of the Internet*, in M. WADE, A. MALJEVIC (Hrsg.), *A War on Terror? The European Stance on a new Threat, Changing Laws and Human Rights Implications*, New York, 2010, 171-219; P. BRUNST, *Terrorism and the Internet*, in M. WADE, A. MALJEVIC (ed.), *A War on Terror?*, cit., 51 e ss.; P. BRUNST., *Legal Aspects of Cyber Terrorism*, in CENTRE OF EXCELLENCE – DEFENCE AGAINST TERRORISM (ed.), *Legal Aspects of Combating Terrorism*, Amsterdam, NATO Science for Peace and Security Series, 2008, 63 e ss.; P. BRUNST, *Use of the Internet by Terrorists – A Threat Analysis*, in CENTRE OF EXCELLENCE – DEFENCE AGAINST TERRORISM (ed.), *Responses to Cyber Terrorism*, Amsterdam, NATO Science for Peace and Security Series, 2008, 34 e ss.

[23] Vedi, anche sulla classificazione dei reati informatici propri e impropri (o comuni), nonché cibernetici in senso stretto e cibernetici in senso lato, L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21 e ss.; L. PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione*

essa previsti, ma anche a tutti i reati per il cui accertamento è necessaria la raccolta della prova elettronica (art. 14 CC)[24].

Sul piano del diritto penale sostanziale, sia le disposizioni della Convenzione *Cybercrime* sia quelle della direttiva europea in materia di attacchi contro i sistemi di informazione, sono da ritenere attuate dal nostro ordinamento.

La l. n. 48 del 2008 ha apportato modifiche al codice penale e all'originario impianto previsto dalla l. n. 597 del 1993 in materia di criminalità informatica.

Da un lato, essa ha ampliato l'area di punibilità anche attraverso una moltiplicazione di fattispecie[25] mentre, dall'altro lato, non ha apportato modifiche alla formulazione originaria di altre norme, mantenendo l'incriminazione anche di condotte non previste dalle fonti sovranazionali ed europee[26], ovvero ha inciso sulla struttura di singole fattispecie, inserendo nuovi elementi[27].

---

*internazionale*, in *Dir. Internet*, 2005, 189 e ss. Dopo la legge di ratifica della Convenzione Cybercrime cfr. L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, 700 e ss.; R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*, in *Dir. pen. Contemporaneo*, 20 settembre 2012.

[24] Il trattato prevede, infatti, sul piano del diritto penale sostanziale, che ogni parte adotti le misure necessarie al fine di sanzionare penalmente diverse fattispecie, quali l'accesso illegale a sistemi informatici e telematici (art. 2 CC), l'intercettazione illegale (art. 3 CC), l'attentato all'integrità dei dati (art. 4 CC), l'attentato all'integrità dei sistemi informatici (art. 5 CC), l'abuso di dispositivi (art. 6 CC), la falsificazione di dati (art. 7 CC), la frode informatica (art. 8 CC), le offese relative alla pornografia minorile (art. 9 CC) nonché le violazioni del diritto d'autore (art. 10 CC). L'art. 12 CC, inoltre, prevede che tali illeciti siano oggetto anche della responsabilità da reato delle persone giuridiche. Sul piano del diritto processuale sono previste, inoltre, specifiche disposizioni in ordine alla conservazione dei dati di traffico telematico ed alla loro comunicazione (artt. 16 e 17 CC); alle misure per la perquisizione ed il sequestro dei dati informatici, nonché per l'accesso ai sistemi informatici in cui sono archiviati dati e informazioni (art. 19 CC); la raccolta in tempo reale dei dati ("real-time collection", art. 20 CC) e per l'intercettazione del contenuto dei dati (art. 21 CC).

[25] Si pensi, in particolare, ai reati in materia di danneggiamento informatico (ex artt. 635 bis e seguenti c.p.), nonché alle nuove previsioni relative al certificatore di firma elettronica (ex artt. 495 bis e 640 quinquies c.p.).

[26] È il caso, ad esempio, dell'art. 615 ter c.p., che sanziona, accanto all'accesso abusivo, anche il mantenimento senza autorizzazione in un sistema informatico (condotta,

*De jure condito*, al fenomeno cyber-terrorismo o ad una delle sue componenti fenomeniche, nelle accezioni sopra riportate, possono trovare applicazione diverse fattispecie incriminatrici.

Si pensi, ad esempio, ad un attacco informatico diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, che integrerebbe il reato di cui all'art. 635 ter c.p.[28], oppure ad un fatto diretto a distruggere, deteriorare o rendere inservibile, anche solo in parte, un sistema informatico di pubblica utilità o ad ostacolarne gravemente il funzionamento, che sarebbe punito dall'art. 635 quinquies c.p.

In entrambi i casi, se tali fatti producono le conseguenze dannose la pena prevista è quella più severa della reclusione da tre a otto anni.

Un'ulteriore ipotesi potrebbe riguardare l'accesso abusivo a sistemi informatici, anche a fini di spionaggio ovvero per sottrarre informazioni strategiche per la sicurezza dello Stato, che configurerebbe quantomeno il reato di cui all'art. 615 ter c.p.

In caso di attività preparatorie, quali potrebbero essere la consegna o la messa a disposizione di *softwares* malevoli al fine di danneggiare illecitamente sistemi informatici, dati o informazioni, ovvero l'intercettazione illecita di comunicazioni informatiche o telematiche fra sistemi per acquisire dati strategici sulla configurazione delle infrastrutture lo-

---

quest'ultima, non prevista dalle fonti sovranazionali ed europee). Cfr. R. FLOR, *Verso una rivalutazione dell'art. 615 ter c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nell'era di Internet*, in *Dir. pen. cont. trim.*, 2012, 126 ss.

[27] Si pensi, a titolo di esempio, all'art. 615 quinquies c.p. e al nuovo dolo specifico. Nella precedente formulazione, infatti, lo "scopo" di danneggiare era oggettivamente legato alla natura del programma e non alla finalità soggettiva dell'agente.

[28] L'art. 6 della l. n. 48 del 2008 ha abrogato i co. 2 e 3 dell'art. 420 c.p., che punivano i fatti diretti a danneggiare o distruggere sistemi informatici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti. La pena era della reclusione da tre a otto anni se del fatto derivava la distruzione o il danneggiamento del sistema, dei dati, delle informazioni o dei programmi, ovvero l'interruzione anche parziale del funzionamento del sistema. Tale previsione è stata, di fatto, sostituita dall'introduzione delle fattispecie di danneggiamento informatico, ex artt. 635 ter e 635 quinquies c.p., che hanno ampliato l'area di punibilità.

giche *target* o, ancora, l'installazione di applicazioni atte ad intercettare tali comunicazioni, potrebbero trovare applicazione, rispettivamente, gli artt. 615 quinquies, 617 quater e 617 quinquies c.p. Se l'intercettazione illecita o l'installazione di apparecchiature atte ad intercettare avesse ad oggetto le comunicazioni fra persone troverebbero applicazione anche i reati informatici c.d. "comuni", previsti dagli artt. 615 bis, 617 e 617 bis c.p.

Non sembrano sussistere, dunque, particolari o gravi lacune, in quanto il nostro ordinamento, almeno nel settore della "criminalità informatica", appare oggi dotato di alcuni minimi strumenti di prevenzione e di contrasto di attività che possono essere inquadrate nel fenomeno cyber-terrorismo.

Un possibile intervento legislativo potrebbe eventualmente riguardare l'impianto sanzionatorio rispetto a fatti particolarmente gravi realizzati con "finalità di terrorismo".

Ad esempio, l'accesso abusivo a sistemi informatici, nella ipotesi aggravata, qualora riguardi sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica, o alla sanità o alla protezione civile, o comunque di interesse pubblico, è punito con la pena della reclusione, rispettivamente da uno a cinque anni e da tre a otto anni. In verità si tratta di attività che mettono in pericolo sistemi sensibili e critici dello Stato, che risultano essere fondamentali, nella società dell'informazione, in settori strategici strettamente connessi alla vita ed al mantenimento della "pace" sociale. L'irrazionalità sanzionatoria è maggiormente evidente se si raffronta tale cornice edittale con quelle previste, ad esempio, per la persona arruolata (ex art. 270 quater c.p.) o in casi di auto-addestramento (ex art. 270 quinquies c.p.)[29].

Il medesimo ragionamento potrebbe riguardare anche i fatti puniti dagli artt. 635 ter e 635 quinquies c.p., in particolare quando deriva, rispettivamente, la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, e la distruzione o il danneggiamento del sistema informati-

[29] Vedi infra, 3.2.

co o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile.

In entrambi i casi la pena è della reclusione da tre a otto anni. Anche ammettendo l'applicazione dell'aggravante della finalità terroristica e di eversione dell'ordine democratico, di cui all'art. 1 d.l. n. 625 del 1979, convertito con la l. n. 15 del 1980 (che comporta un aumento di pena della metà, salvo che la circostanza sia elemento costitutivo del reato), permarrebbero i dubbi connessi alla irrazionalità sanzionatoria[30].

Nell'ipotesi di cui al co. 2 dell'art. 270 quinquies, infatti, anche nel solo caso di "auto-addestramento", la pena prevista è quella della reclusione da cinque a dieci anni.

### *3.2. Cyber-terrorismo e legislazione anti-terrorismo*

L'attuale disciplina interna anti terrorismo, come modificata dagli ultimi interventi normativi del 2015 e del 2016, può trovare applicazione anche a fatti riconducibili al fenomeno cyber-terrorismo, pur con non poche difficoltà ermeneutiche.

Il nuovo art. 270 quinquies c.p. sanziona *chi addestra*,

> o comunque fornisce istruzioni sulla preparazione o sull'uso di materiali esplosivi, di armi da fuoco o di altre armi, di sostanze chimiche o batteriologiche nocive o pericolose, nonché di ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo.

Punisce però anche sia *chi viene addestrato* – nonché, secondo una criticabile interpretazione estensiva dell'art. 270 quinquies c.p., nella

[30] Sull'applicazione di tale aggravante in casi recenti vedi A. VALSECCHI, *I requisiti oggettivi della condotta terroristica ai sensi dell'art. 270 sexies c.p. (prendendo spunto da un'azione dimostrativa dell'Animal Liberation Front)*, in *Diritto penale cont.*, 21 febbraio 2013. Cfr. inoltre F. VIGANÒ, *Terrorismo di matrice islamico-fondamentalista e art. 270-bis nella recente esperienza giurisprudenziale*, in *Cass. pen.*, 2007, 3981 e ss.; A. VALSECCHI, *Il problema della definizione di terrorismo*, in *Riv. it. dir. proc. pen.*, 2004, 1127 e ss. In giurisprudenza, fra le decisioni più recenti, vedi Cass., sez. I, pen., 6 ottobre 2015, n. 47489; Cass., sez. V pen., 13 marzo 2012, n. 25428; Cass., sez. V pen., 23 febbraio 2012, n. 12252; Cass., sez. I pen., 11 febbraio 2010, n. 8069.

sua formulazione originaria, chi si "autoaddestra", perché "persona addestrata" a prescindere dall'interazione con un addestratore – sia *chi solo si informa*, *"acquisisce istruzioni"* e poi realizza qualsiasi comportamento, purché si tratti di comportamenti univocamente finalizzati alla commissione delle condotte di cui all'art. 270 sexies c.p.[31].

La fattispecie sembrerebbe astrattamente applicabile, quindi, sia a colui che, con "finalità di terrorismo", attraverso la rete e le sue infinite potenzialità fornisce informazioni (si pensi solo, ad esempio, a video caricati dagli utenti in *youtube* o altri *social media* contenenti istruzioni per creare in modo artigianale un ordigno esplosivo), sia a chi, tramite ricerche in Internet, assume informazioni (ad esempio per costruire esplosivi o per realizzare armi da fuoco tramite stampe 3D), se pone in essere quei «comportamenti univocamente finalizzati alla commissione delle condotte di cui all'art. 270-*sexies* c.p.».

Secondo una parte della dottrina[32] tale ultima "clausola" dovrebbe evitare la punibilità di fatti diretti alla mera acquisizione di informazioni.

Ma la tesi potrebbe apparire incoerente con le intenzioni del legislatore di sanzionare l'auto-addestramento, in quanto si punirebbe il compimento di condotte con finalità di terrorismo, rispetto alle quali proprio il reperimento delle istruzioni rappresenterebbe un antefatto.

La fattispecie *de qua*, però, fa riferimento a qualsiasi "comportamento" («avendo acquisito, anche autonomamente, le istruzioni per il compimento degli atti di cui al primo periodo», ossia anche «ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali») soggettivamente rivolto a commettere delitti con finalità di terrorismo, consentendo l'incriminazione di qualsiasi, pur remoto, atto preparatorio quando sussista tale fine.

---

[31] Cfr. R. WENIN, *L'addestramento per finalità di terrorismo alla luce delle novità introdotte dal d.l. 7/2015. Una riflessione comparata sulle tecniche di descrizione della fattispecie muovendo dalla sentenza del Bundesgerichtshof tedesco StR 243/13*, in *Dir. pen. contemporaneo*, 3 aprile 2015. Prima del d.l. del 2015 vedi A. VALSECCHI, *L'accertamento del (doppio) dolo specifico nel reato di addestramento ad attività con finalità di terrorismo*, in *Cass. pen.*, 2012, 903 e ss.

[32] Vedi di recente M. PELISSERO, *Contrasto al terrorismo*, cit., 99 ss.

Poiché la finalità di terrorismo di cui all'art. 270 sexies c.p. è notoriamente ampia ed indeterminata, ciò implica un'espansione della punibilità, finanche della raccolta di informazioni nel *web* o tramite il *web* – se univocamente finalizzata alla commissione delle condotte di cui all'art. 270 sexies – che andrebbe a confermare, invece, l'impressione di una esasperazione repressiva[33].

La stessa propaganda di viaggi attraverso Internet (in *forum*, *blog*, siti *web*, *mailing list*), o l'organizzazione (che può realizzarsi interamente in Internet), anche in Paesi in cui vi è la certezza di un legame con gruppi terroristici, costituiscono di per sé una condotta neutra. Esse assumono rilevanza penale solo se sono finalizzate al compimento delle condotte con finalità di terrorismo (ex art. 270 quater-1 c.p.).

L'esigenza di un accertamento concreto impegna il giudicante in un compito ed una attività complessi, soprattutto se il legislatore sanziona tali fatti «fuori dei casi di cui all'art. 270 bis» o, come nell'ultima ipotesi riportata, «fuori dei casi di cui agli artt. 270 bis e 270 quater» c.p.

È apprezzabile lo sforzo volto a ricercare una maggiore selettività a fronte di condotte potenzialmente neutre, rispetto alle quali la "finalità di terrorismo" rischierebbe di assumere un ruolo assorbente.

Tale finalità, dunque, dovrà trovare concreto riscontro in ulteriori elementi oggettivi che manifestino o esprimano l'idoneità di quei comportamenti e, al contempo, la pericolosità dell'informazione dovrà esse-

[33] Secondo una parte della dottrina "esasperazione" tale da equiparare il livello sanzionatorio a quello previsto per la partecipazione ad associazione con finalità di terrorismo. Vedi in questo senso A. CAVALIERE, *Considerazioni critiche*, cit. Lo stesso inserimento del requisito legale di "comportamenti univocamente finalizzati" alle attività con finalità terroristiche per punire l'auto-addestramento del c.d. lupo solitario (nuovo art. 270 quinquies dopo riforma del d.l. n. 7 del 2015), sembra limitare correttamente la fattispecie a un principio di materialità, altrimenti assente nell'auto-addestramento informativo. Però univocamente finalizzati non significa oggettivamente idonei. E la sua pena, come peraltro anche quella del semplice addestrato "vero" e dell'addestratore che non abbiano compiuto quei comportamenti finalizzati univocamente, è la stessa del partecipe interno: da cinque a dieci anni di reclusione. Un'equiparazione sanzionatoria che dimostra il livellamento punitivo di associato, addestratore, addestrato e auto-addestrato esterno indipendente Così M. DONINI, *Terrorismo e ruolo della giurisdizione. Dal codice delle indagini preliminari a quello postdibattimentale*, in *Questione e Giustizia* (speciale), 2016, 138 ss.

re valutata guardando non solo alla sua "natura", ma anche al contesto complessivo in cui è inserita ed al modo in cui è veicolata[34].

Altra è la questione relativa alla scelta del legislatore italiano di sanzionare la condotta di "acquisizione", rispetto a quelle, ad es., di "ottenere", "procurarsi", "detenere".

La fattispecie può essere classificata, sul piano sistematico, fra i reati informatici c.d. "impropri" o "comuni", per i quali gli strumenti informatici o telematici costituiscono *solo una* delle modalità per la commissione dell'illecito.

Di conseguenza l'interpretazione della condotta di "acquisire" deve essere adattabile anche, ma non solo, al contesto tecnologico.

Le informazioni, infatti, possono essere reperite, ad es., attraverso giornali, riviste specializzate o manuali. Se il tentativo del legislatore era quello di meglio delimitare l'area di punibilità, la condotta in oggetto costituisce un ante fatto che, di per sé, non assume rilevanza penale, se non nel momento in cui vengono posti in essere quei comportamenti "univocamente finalizzati".

Pertanto, la norma sembra presupporre che il fulcro del disvalore sociale del fatto debba essere concentrato, in primo luogo, sulla astratta idoneità delle istruzioni per porre in essere quegli atti (di cui al primo periodo); in secondo luogo, sulla loro concreta comprensione, sul piano intellettivo, da parte dell'autore, perché solo in questo modo egli potrebbe porre in essere quei fatti finalizzati alla commissione delle condotte di cui all'art. 270 sexies; infine, sul loro utilizzo per porre in essere comportamenti concreti univocamente finalizzati alla commissione

[34] In giurisprudenza vedi ad es. Cass., sez. I pen., 9 settembre 2015, n. 40699, in cui i giudici hanno affermato che si deve escludere che nell'ipotesi prevista dall'art. 270 quater sia necessario l'inquadramento dell'arruolato in una vera e propria struttura di tipo militare, dovendosi invece ritenere, anche alla luce dell'espresso riferimento operato dalla norma incriminatrice alle finalità di terrorismo, che il concetto di "arruolamento" corrisponda a quello di "ingaggio", inteso come il raggiungimento di un "serio accordo" tra il soggetto che propone il compimento, in forma organizzata, di più atti di violenza o di sabotaggio, con finalità di terrorismo, ed il soggetto chiamato ad aderire ad una tale proposta; raggiungimento, quello anzidetto, che segna pertanto il momento consumativo del reato; il che, peraltro, non esclude la configurabilità del tentativo punibile, ove il proponente, pur ponendo in essere una condotta idonea ed univocamente diretta ad ottenere l'adesione del destinatario, non consegua tale risultato.

delle condotte di cui all'art. 270 sexies. Né può valere un parallelismo con i reati in materia di pedopornografia e, in specie, con l'art. 600 quater c.p. In questi casi, infatti, il disvalore del fatto è concentrato sull'oggetto della condotta, e non su quest'ultima, di natura neutra. Viceversa, l'art. 270 quinquies punisce l'acquisizione – ed eventualmente anche la detenzione, la quale presuppone logicamente il "procurarsi" o l'"acquisire" – delle informazioni solo se si realizzano i citati comportamenti successivi[35].

Pertanto, la scelta politico-criminale appare, su questo aspetto, condivisibile, in quanto la condotta è astrattamente idonea ad attrarre varie accezioni, quali l'acquisto e il possesso (in senso materiale), il procurarsi o il detenere informazioni e istruzioni (in senso immateriale), nonché l'assimilazione intellettuale, purché sussista quel decorso causale fra informazioni, comprensione, assimilazione e utilizzo.

Concretamente, dunque, la semplice detenzione o memorizzazione, anche non temporanea, nella memoria di un sistema o di un qualsiasi *device*, di istruzioni relative, ad es., alla fabbricazione di un ordigno esplosivo o sull'uso di armi da fuoco, ovvero l'accesso a pagine Internet che contengono quelle informazioni, non assumono di per sé rilevanza penale. Possono costituire un indizio di un comportamento "pericoloso", ma non di per sé sufficiente per integrare gli elementi costitutivi della fattispecie di cui all'art. 270 quinquies c.p.

Non è esente da critiche nemmeno il co. 2 all'art. 270 quater c.p., in tema di arruolamento per finalità di terrorismo, che sancisce perentoriamente la punibilità della "persona arruolata". In questo caso si assiste ad una rinuncia alla descrizione del fatto, tanto che la fattispecie potrebbe essere astrattamente applicabile in casi in cui, in difetto di altri riscontri oggettivi, un soggetto esprima il proprio impegno, eventual-

[35] Non è condivisibile dunque, a parere di chi scrive, la distinzione critica fra condotte, effettuata recentemente da una parte della dottrina (R. WENIN, *Una riflessione comparata sulle norme in materia di addestramento per finalità di terrorismo*, in *Diritto penale contemporaneo*, 23 gennaio 2017, 31 ss.), basata su argomentazioni sistemiche legate a fattispecie, quali quella di cui all'art. 600 quater c.p., o a condotte, quali quelle di procurarsi, ottenere e detenere, previste in contesti diversi e in considerazione delle diverse *ratio* di tutela.

mente ripetuto in *blog*, siti *web*, profili di *social networks*, a realizzare un attentato terroristico.

Lo stesso art. 270 bis c.p. punisce chiunque promuove, costituisce, organizza, dirige o finanzia associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico[36].

Nell'attuale società di Internet soprattutto la promozione e l'organizzazione di tali associazioni avviene *online* con infinite soluzioni tecniche, anche tramite *social networks* e *social media*. Ovviamente la struttura organizzativa deve presentare un grado di effettività tale da rendere possibile l'attuazione del progetto criminoso e da giustificare la valutazione legale di pericolosità, correlata alla idoneità della struttura al compimento della serie di reati per la cui realizzazione l'associazione è stata istituita. In tal caso lo strumento tecnologico può costituire uno dei molteplici mezzi per la commissione del reato.

Sul piano del diritto penale sostanziale, è altresì criticabile la scelta del legislatore relativa alla previsione delle circostanze aggravanti speciali di tipo oggettivo (artt. 1 co. 3 lett. b e soprattutto art. 2 co. 1 del citato d.l. anti terrorismo), che prevedono un aumento di pena se il fatto è commesso attraverso l'utilizzo di strumenti informatici. Tali aggravanti sono previste dagli artt. 270 quinquies, 302 e 414 c.p.

La scelta politico-criminale è criticabile non tanto per la selezione delle fattispecie penali in questione, bensì per prevedere l'aumento di pena per fatti che, nell'attuale società dell'informazione, trovano in Internet e nelle nuove tecnologie un *mezzo* o uno *strumento non certo straordinario* di commissione di reati.

Da un lato, tale scelta è apparentemente giustificata dalle potenzialità offerte dalla rete, considerata particolarmente insidiosa per la diffusività incontrollabile del messaggio terroristico e per la facilità di reperire informazioni e risorse.

Dall'altro lato, però, le aggravanti in questione non sembrano consentire al Giudice una valutazione di maggiore diffusività/pericolosità, grazie alla rete ed alle tecnologie, del messaggio a "stampo terroristi-

[36] Cfr. R. BARBERINI, *"Sovversivi, non terroristi": la Corte di Cassazione offre una rivoluzionaria interpretazione dell'art. 270-bis*, in *Cass. pen.*, 2012, 3347 e ss.

co", essendo prevista *ex lege* una presunzione di maggiore offensività del mezzo impiegato, che prescinde dalla verifica della concreta idoneità della condotta a integrare o provocare la commissione dei delitti.

Più in particolare, l'aumento di pena previsto dall'art. 270 quinquies c.p. riguarda il *soggetto che addestra* o *istruisce*. Per cui è da escludere che la circostanza aggravante si applichi al soggetto destinatario dell'attività di addestramento o istruzione, o a colui che autonomamente acquisisce le istruzioni.

Questa scelta politico-criminale appare singolare. Sul piano penale dovrebbe essere rilevante l'utilizzo, da parte di un soggetto, di tali strumenti per la commissione del reato. Non si comprende, dunque, il motivo per cui il legislatore abbia previsto una sostanziale e formale omologazione sanzionatoria per chi addestra, viene addestrato e reperisce in via autonoma le informazioni, probabilmente basata sulla valutazione del disvalore sociale della condotta, mentre abbia limitato l'aumento di pena solo a colui che addestra o istruisce. Le potenzialità offerte dalle tecnologie, infatti, svolgono il medesimo ruolo in tutti i casi.

Nell'attuale società di Internet l'uso di strumenti informatici, in particolare per diffondere idee, comunicare o reperire informazioni non può certo dirsi né un'attività di carattere straordinario o eccezionale, né un comportamento di per sé "pericoloso".

La scelta politico-criminale, dunque, sembra operare una inversione del rapporto regola-eccezione, con il rischio di demonizzare le nuove tecnologie rispetto a tradizionali strumenti di comunicazione o di diffusione, soprattutto *in subiecta materia*, in cui la valutazione in concreto dell'offesa avrebbe potuto svolgersi servendosi degli ordinari criteri di commisurazione della pena (ex art. 133 c.p.), considerando le cornici edittali previste dagli artt. 270 quinquies, 302 e 414 c.p.

Con la l. n. 153 del 2016[37] il legislatore italiano ha introdotto ulteriori fattispecie incriminatrici, fra cui quella prevista dal nuovo art. 270 quinquies-1 (Finanziamento di condotte con finalità di terrorismo)[38].

[37] La l. 28 luglio 2016, n. 153 ha introdotto norme per il contrasto al terrorismo, dando altresì ratifica: della Convenzione del Consiglio d'Europa per la prevenzione del terrorismo (Varsavia il 16 maggio 2005); della Convenzione internazionale per la soppressione di atti di terrorismo nucleare (New York il 14 settembre 2005); del Protocollo di Emendamento alla Convenzione europea per la repressione del terrorismo (Strasbur-

Le organizzazioni terroristiche sono state tra le prime a cogliere le opportunità offerte dalla società dell'informazione, che ha trasformato il mondo finanziario e l'attività economica. Tale trasformazione ha influito sui mezzi di raccolta, gestione e trasferimento delle risorse, anche grazie alla rete ed alla sua forza "di aggregazione", che facilita i meccanismi di finanziamento e auto-finanziamento.

Il *funding*, ossia la capacità di finanziamento da parte dei gruppi terroristici deve essere misurata attraverso i processi non solo di *money laundering* e *cyberlaundering*, ma anche di *money dirtying*[39].

Quest'ultimo riguarda attività di per sé lecite, che sempre più spesso sfruttano le potenzialità e le utilità di Internet i cui introiti vengono, anche solo in parte, devoluti o utilizzati per finanziare attività terroristiche. La rete e il *deep web*, infatti, facilitano non solo i meccanismi di pubblicità e di diffusione di informazioni – utili ad attrarre "benefattori" – ma anche quelli di ricerca, raccolta, gestione, occultamento e impiego dei fondi, nonché il loro trasferimento a enti, gruppi o organizza-

---

go il 15 maggio 2003); della Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo (Varsavia il 16 maggio 2005); del Protocollo addizionale alla Convenzione del Consiglio d'Europa per la prevenzione del terrorismo (Riga il 22 ottobre 2015).

[38] La disposizione prevede: «Chiunque, al di fuori dei casi di cui agli articoli 270-bis e 270-quater-1, raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo di cui all'articolo 270-sexies è punito con la reclusione da sette a quindici anni, indipendentemente dall'effettivo utilizzo dei fondi per la commissione delle citate condotte. Chiunque deposita o custodisce i beni o il denaro indicati al primo comma è punito con la reclusione da cinque a dieci anni».

[39] Per una definizione di *cyberlaundering*, sul piano criminologico, basti il rinvio, in questa sede, a D.A. LESLIE, *Legal Principles for Combatting Cyberlaundering*, New York, 2014, 55 ss. Cfr. altresì con riferimento al *money dirtying*, U. TURKSEN, *Implications of anti-money laundering law for accountancy in European Union – a comparative study*, in N. RYDER, U. TURKSEN, S. HASSLER (eds.), *Fighting Financial Crimes in the Global Economic Crisis*, New York, 2015, 75 ss. Vedi anche R. DURRIEU, *Rethinking Money Laundering and Financing of Terrorism in International Law*, Leiden-Boston, 2013, 104 ss., 151 ss. Fa riferimento alla distinzione fra *money laundering* e *money dirtying* anche A. BALSAMO, *Nuove norme sul procedimento di prevenzione*, in R.E. KOSTORIS, R. ORLANDI (cur.), *Contrasto al terrorismo interno e internazionale*, Torino, 2006, in specie 189 s. (nota 21).

zioni di stampo terroristico, situati soprattutto fuori dal territorio nazionale.

I fenomeni del riciclaggio o dell'impiego di denaro di provenienza delittuosa in attività economiche o finanziarie, invece, che già possono assumere autonoma rilevanza penale, sono strettamente legati a quello terroristico quando la sostituzione o trasferimento di denaro, beni o altre utilità provenienti da delitto, ovvero il compimento di altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, ovvero l'impiego di denaro, beni o altre utilità provenienti da delitto in attività economiche o finanziarie, avvengono per "sostenere" l'attività terroristica.

Nell'assetto normativo previgente la punibilità delle condotte di finanziamento al terrorismo poteva essere ricondotta al co. 1 dell'art. 270 bis c.p. (che punisce il finanziamento di associazioni con finalità di terrorismo) e, più recentemente, all'art. 270 quater-1 c.p. (che sanziona la condotta di chi finanzia viaggi in territorio estero finalizzati al compimento delle condotte con finalità di terrorismo).

L'attuale disciplina di cui all'art. 27 quinquies-1, introdotta con la novella del 2016, appare ispirata all'art. 2 della Convenzione ONU per la soppressione del finanziamento al terrorismo (New York, 9 dicembre 2001), in quanto ha previsto la possibilità di colpire il fatto di chi raccoglie, eroga o mette a disposizione beni o denaro che siano destinati ad essere in tutto o in parte utilizzati per il compimento di «condotte con finalità di terrorismo»[40].

In primo luogo, la disposizione precisa che tali comportamenti sono puniti «indipendentemente dall'effettivo utilizzo dei fondi per il compimento delle citate condotte».

In secondo luogo, e in ogni caso, la nuova fattispecie non distingue fra provenienza delittuosa (o illecita) e non delittuosa (o illecita) dei beni o del denaro, punendo la raccolta, l'erogazione e la messa a disposizione di questi «in qualunque modo realizzati», purché siano destinati a essere totalmente o parzialmente utilizzati per il compimento delle condotte con finalità di terrorismo.

[40] Cfr. R. BERTOLESI, *Ancora nuove norme in materia di terrorismo*, in *Diritto penale contemporaneo*, 19 ottobre 2016.

In terzo luogo assume rilevanza penale anche solo l'attività di deposito o di custodia di tali beni e denaro.

Se tali fatti sono realizzati attraverso la rete e le nuove tecnologie possono essere attratti nella sfera applicativa della nuova incriminazione in quanto, anzitutto, la struttura della fattispecie è a forma libera e, in secondo luogo, la sua *ratio* appare individuabile proprio nel voler sanzionare in via autonoma qualsiasi comportamento di «fiancheggiamento o sostegno del terrorismo internazionale»[41].

L'art. 270 quinquies-1 trova comunque applicazione fuori dai casi previsti dagli artt. 270 bis e 270 quater-1 c.p. Per cui la nuova incriminazione potrebbe andare a colmare gli spazi lasciati vuoti da queste ultime disposizioni come, ad esempio, le ipotesi di finanziamento di "lupi solitari", ovvero quando non sia raggiunta la prova dell'inserimento del soggetto finanziato in un'associazione terroristica o, ancora, nelle ipotesi in cui il finanziatore non conosca l'affiliazione del soggetto finanziato ad un'organizzazione terroristica, salvo che le condotte di finanziamento non siano dirette all'organizzazione di viaggi con finalità di terrorismo[42].

Anche in questo caso il legislatore, dunque, conferma la preoccupazione e l'intenzione di reprimere atti preparatori di condotte con finalità di terrorismo e di assicurare la più ampia punibilità di quei comportamenti «indipendentemente dall'effettivo utilizzo dei fondi».

Il d.l. anti-terrorismo del 2015, infine, ha apportato modifiche all'art. 7 bis co. 2 (Sicurezza telematica) d.l. n. 144 del 2005, convertito, con modificazioni, dalla l. n. 155 del 2005. Tale disposizione oggi prevede che, per assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale e per la prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo condotte con i mezzi informatici, gli ufficiali di polizia giudiziaria (appartenenti agli organismi investigativi di Polizia di Stato, Arma dei Carabinieri specializzati nell'attività di contrasto al terrorismo e all'eversione e della Guardia di Finanza competenti nelle attività

[41] Vedi «Norme per il contrasto al terrorismo, nonché ratifica ed esecuzione di convenzioni internazionali in materia». A. C. 3303-A. Dossier n. 368/1 – Elementi per l'esame in Assemblea 22 gennaio 2016, 2.

[42] Cfr. R. BERTOLESI, *Ancora nuove norme*, cit.

di contrasto al finanziamento al terrorismo anche internazionale) possono svolgere le attività di cui all'art. 4, co. 1 e 2, della l. n. 438 del 2001 – attività sotto copertura anche per attivare o entrare in contatto con soggetti e siti nelle reti di comunicazione – oltre a quelle di cui all'art. 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale.

L'estensione di tali attività investigative appare opportuna non solo per il contrasto e la prevenzione del terrorismo "tradizionale", che può sfruttare le nuove tecnologie nella preparazione, compresa la comunicazione fra singoli o gruppi organizzati, e nell'esecuzione di attacchi terroristici, ma anche per la lotta al cyber-terrorismo («per assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale»)[43], al fine di prevenire attacchi a sistemi informatici e di comunicazione, nonché banche dati o strutture logiche sensibili dello Stato.

Il legislatore italiano purtroppo non ha colto l'occasione per prevedere nuovi mezzi tecnologici di ricerca della prova come, ad esempio, le c.d. perquisizioni *online* o la *data retention*[44], adattabili alle esigenze

[43] In Italia con il DPCM 24 gennaio 2013, è stata adottata la «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale» (G.U. 19 marzo 2013, n. 66) avente l'obiettivo di accrescere le capacità del nostro paese di confrontarsi con le minacce provenienti dallo spazio cibernetico anche attraverso la riorganizzazione dell'architettura istituzionale del settore, considerata disorganica ed inefficiente. Per la prima volta si è proceduto alla definizione normativa di concetti chiave, quali quelli di «spazio», «sicurezza», «minaccia», «evento cibernetico» e, nel contempo, di «allarme» e di «situazione di crisi». Il dibattito sulla c.d. *cyber-security* ha origine negli Stati Uniti negli anni '70 per rispondere all'innovazione tecnologica ed ai cambiamenti delle condizioni geo-politiche nel periodo della guerra fredda. Cfr. ampiamente S. ADAMS, M. BROKX, L. DALLA CORTE, M. GALIC, K. KALA, B.J. KOOPS, I. SKORVÁNEK, *The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK*, Tilburg, 2015, in specie 15 ss.

[44] La possibilità di utilizzare specifici *softwares* per condurre attività di indagine o di *intelligence* è stata per la prima volta introdotta in Germania, in particolare nel *Land Nord Rhein Westfalen*, dove attraverso una modifica della Legge sulla protezione della Costituzione del *Land* si autorizzava un organismo di intelligence a "protezione della costituzione" (*Verfassungsschutzbehörde*) ad effettuare due tipi di indagine: il monitoraggio e la ricognizione segreti di Internet e l'accesso segreto a sistemi informatici (§ 5 Abs. 2, n. 11). Come noto, sulla questione è intervenuta nel 2008 la Corte costituzionale

tedesca che, pur dichiarando la suddetta normativa incostituzionale in quanto non rispettosa dei principi di proporzionalità e determinatezza, non ha escluso in assoluto l'ammissibilità di tale strumento di indagine. Ritenendo insufficienti le garanzie offerte dalle norme costituzionali a tutela della segretezza delle telecomunicazioni (art. 10 *Grundgesetz*, d'innanzi GG) e dell'inviolabilità del domicilio (art. 13 GG) e, altresì, del diritto all'autodeterminazione informativa, il Bundesverfassungsgericht ha preso atto dell'esistenza di un nuovo diritto fondamentale "alla garanzia della segretezza e integrità dei sistemi informatici" (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). Un diritto di rango costituzionale, ricavato da quella sorgente di diritti inviolabili che è la *Menschenwürde* (artt. 1, comma 1 e 2, comma 1 GG) BVerfG 370/07 - 595/07, 27.02.2008, in CR, 2008, 306 e ss. Vedi il primo commento alla sentenza di R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. trim. dir. pen. ec.*, 2009, 695 e ss.; R. FLOR, *La tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del Bundesverfassungsgericht e della Curtea Constitucionala su investigazioni ad alto contenuto tecnologico e data retention*, in L. PICOTTI, F. RUGGIERI (cur.), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, 32-49. Recentemente la Spagna, con la *Ley Orgánica* 13/2015, di modifica della *Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica* ha introdotto il c.d. *Registros remotos sobre equipos informáticos* (art. 588 septies a), che permette al giudice competente di autorizzare l'applicazione di un software specifico che consenta l'accesso segreto ad un sistema informatico purché venga utilizzato per il perseguimento dei gravi reati indicati dalla stessa disposizione, fra cui sono previsti quelli a stampo terroristico. Il co. 2 della stessa disposizione prevede le specifiche garanzie da adottare ed i contenuti del provvedimento del giudice. Vedi R. FLOR, *Il contrasto al terrorismo*, cit.; prima della riforma spagnola cfr. F. IOVENE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont. trim.*, 2014, 329 ss. Sul c.d. captatore informatico vedi Cass. pen., Sezioni Unite, 28 aprile 2016, n. 26889, con nota di G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in *Diritto penale contemporaneo*, 7 ottobre 2016; in *Arch. nuova proc. pen.*, 2017, 76 e ss. con nota di A. CAMON, *Cavalli di troia in Cassazione*; in *Cass. pen.*, 2016, 2274-2288, con nota di A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*; in *Dir. inf.*, 2016, 88 ss., con nota di G. CORASANITI, *Le intercettazioni "ubiquitarie" e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*. Cfr. anche F. CAJANI, *Odissea del captatore informatico*, in *Cass. pen.*, 2016, 4140 ss. La vicenda è complessa. Le SU, in sintesi, hanno affermato che «deve escludersi la possibilità di compiere intercettazioni nei luoghi indicati dall'art. 614 c.p. *[con il captatore]*, al di fuori della disciplina derogatoria per la criminalità organizzata di cui all'art. 13 d.l. n. 152 del 1991, convertito in

repressive e preventive di attività criminose che trovano nel *cyberspace* un ambiente ideale di manifestazione, ovvero nelle tecnologie un mezzo privilegiato per la loro realizzazione.

La regolamentazione di nuovi mezzi investigativi ad «alto contenuto tecnologico»[45] non può prescindere dal bilanciamento con i diritti fon-

---

l. n. 203 del 1991, non potendosi prevedere, all'atto dell'autorizzazione, i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto del presupposto, previsto dall'art. 266, comma 2, c.p.p., che in detto luogo "si stia svolgendo l'attività criminosa"». È invece «consentita la captazione nei luoghi di privata dimora ex art. 614 c.p., pure se non singolarmente individuati e se ivi non si stia svolgendo l'attività criminosa, per i procedimenti relativi a delitti di criminalità organizzata, anche terroristica, secondo la previsione dell'art. 13 d.l. n. 152 del 1991». Per i procedimenti relativi a delitti di criminalità organizzata «devono intendersi quelli elencati nell'art. 51, co. 3-bis e 3-quater, c.p.p. nonché quelli comunque facenti capo a un'associazione per delinquere, con esclusione del mero concorso di persone nel reato». Su tale vicenda vedi il *Confronto di idee su: "I nuovi equilibri nella tutela della* privacy*"*, in *Archivio penale*, 2016, 309-365, con contributi di Alfredo Gaito e Sandro Fùrfaro, Alberto Cisterna, Leonardo Filippi e Lorenzo Picotti. È oggi in discussione un d.d.l. in subiecta materia (Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario – A.S. n. 2067 e connessi-A/2016 – cfr. Nota breve, Servizio Studi del Senato, n. 126/2016). Sulla lunga e complessa questione relativa, invece, alla *data retention* si consenta di rinviare a R. FLOR, *La giustizia penale nella rete? Tutela della riservatezza versus interesse all'accertamento e alla prevenzione dei reati nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in R. FLOR, D. FALCINELLI, S. MARCOLINI (cur.), *La giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di Internet*, Milano, 2015, 153 e ss.; R. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont. trim.*, 2/2014, 178 ss.; R. FLOR, *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?*, in G. RESTA, V. ZENO ZENCOVICH (cur.), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015, 223 ss. Cfr. S. SIGNORATO, *Contrasto al terrorismo e data retention: molte ombre e poche luci*, in R.E. KOSTORIS, F. VIGANÒ (cur.), *Il nuovo "pacchetto"*, cit., 75 ss.

[45] L'espressione trae spunto da R. FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention*, in *Ciberspazio e Diritto*, vol. 11, n. 2, 2010, 359-392.

damentali dell'individuo. Tale bilanciamento presuppone l'individuazione di elevati standard comuni o condivisibili dagli Stati, almeno a livello europeo, che devono confrontarsi con le esigenze di accertamento e di ricerca della prova ed il rispetto anche di "nuove" manifestazioni dei diritti inviolabili dei cittadini quali, ad esempio, il diritto all'integrità, sicurezza e riservatezza dei sistemi informatici ed il diritto all'autodeterminazione informativa, da elevare ad espressioni di "tradizionali" diritti fondamentali, in particolare da ricondurre alle manifestazioni dei diritti della personalità[46].

## *4. Riflessioni conclusive*

Il cyber-terrorismo costituisce un fenomeno ibrido al quale possono trovare applicazione, in Italia, diverse fattispecie penali, inquadrabili sia fra i reati informatici sia fra quelli specificatamente introdotti per contrastare il terrorismo.

Con riferimento alla legislazione anti terrorismo l'attenzione del legislatore è stata progressivamente incentrata sulla necessità di una risposta preventiva, che controlli alla radice le fonti di rischio[47] attraverso un percorso che sembra portare ad un «diritto penale al limite»[48].

La gravità della minaccia terroristica sembra imporre, effettivamente, un arretramento della soglia di rilevanza penale, sanzionando condotte meramente prodromiche.

La disciplina italiana, se applicata al fenomeno cyber-terrorismo, sembra però sconfinare verso una demonizzazione della rete e degli strumenti informatici, che rischia di limitare in modo sproporzionato le libertà individuali costituzionalmente protette.

Le tecnologie sono figlie legittime della società dell'informazione, in cui gli strumenti informatici e la rete dominano ogni campo della vita umana, determinando cambiamenti epocali sul piano non solo sociale, ma anche economico, culturale e politico.

---

[46] Cfr. R. FLOR, *Il contrasto al terrorismo*, cit.

[47] M. DONINI, *Sicurezza e diritto penale*, in *Cass. pen.*, 2008, 3561.

[48] L'espressione prende spunto da M. PELISSERO, *Contrasto al terrorismo*, cit., 99 ss.

> La società effettivamente possiede una oggettiva fattualità, e la società è davvero costruita da un'attività che esprime significati soggettivi […]. Durkheim sapeva la seconda cosa, come anche Weber sapeva la prima[49].

In altri termini, per comprendere i processi di costruzione sociale della realtà occorre partire dalle basi: ad esempio, dal fatto che esiste una realtà che ci circonda e che diamo per scontata.

La "realtà" della società di Internet è complessa e, probabilmente, caratterizza i "contesti sociali", nella loro concezione tradizionale, perché, a differenza dell'uomo, le tecnologie parlano linguaggi comuni, anche se possono essere espressi in molteplici modi diversi, e sono dominate dalla regola tecnologica, che deve essere comprensibile ai sistemi informatici ed agli applicativi, e non all'uomo.

*In primis*, il "contesto ideologico" in cui si può muovere una persona nel *deep web* o nel *web*, attraverso *social networks* e *social media*, ovvero per la ricerca o la diffusione di informazioni *on-line*, esprime una libertà costituzionalmente garantita, che si manifesta tramite strumenti che amplificano in modo indefinito la potenzialità comunicativa e diffusiva.

In secondo luogo, il "contesto tecnologico moderno" ha contribuito al trasferimento del proprio "privato" nello "spazio pubblico", con la conseguenza di rendere sfuggente e "liquida" la distinzione stessa fra privato e pubblico, soprattutto per il volume di informazioni che vengono riversate nei *social networks*, nel *web* o attraverso di essi[50]. Un uragano di dati che spesso sono espressione della personalità dell'individuo, perché indicano inclinazioni politiche o religiose, sessuali o sullo stato di salute, la cui potenzialità conoscitiva è estesa dalla tecnologia.

In terzo luogo, il "contesto giuridico" dovrebbe comprendere la regola tecnologica per poter disciplinare il suo utilizzo, le sue modalità applicative o i suoi effetti nella società.

---

[49] Vedi P.L. BERGER, T. LUCKMANN, *The Social Construction of Reality*, New York, 1966, 8 ss.

[50] L'espressione trae spunto dall'opera di Z. BAUMAN, D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, Roma, 2015.

In quarto luogo, nel "contesto delle scelte politico-criminali" o, meglio, nella conformazione del diritto penale è in gioco il rapporto fra la sfera dei diritti e delle libertà individuali e quella dei poteri statuali di punire. Il diritto penale tutela quei diritti e quelle libertà e, al contempo, li limita per la tutela di altri beni giuridici.

Un'arma a doppio taglio,[51] che esprime il problema della stessa legittimazione del diritto punitivo. Proprio nelle fattispecie a struttura fortemente anticipata si annida il pericolo di raggiungere il confine della sua delegittimazione.

L'odierno diritto penale di contrasto al terrorismo, applicabile in parte al fenomeno cyber-terrorismo, come si è detto, è caratterizzato da un sensibile arretramento della soglia di punibilità.

Nel momento in cui, però, le condotte preparatorie sono punite, ad esempio, «al di fuori dei casi di cui all'art. 270 bis», come avviene per gli artt. 270 quater, 270 quater-1, 270 quinquies e 270 quinquies-1, le esigenze probatorie si affievoliscono, con il rischio concreto di una invasione e limitazione sproporzionata dei diritti fondamentali e, più in specifico, in taluni casi, della libera manifestazione del pensiero[52].

L'interprete assume, pertanto, un ruolo fondamentale per evitare il pericolo che il diritto penale del fatto si trasformi in diritto penale d'autore e che l'arretramento della soglia di punibilità porti allo sconfinamento verso la repressione di forme di manifestazione del pensiero[53].

In concreto, non dovrebbe essere sufficiente, ad esempio, una mera attività di proselitismo ed indottrinamento, anche se finalizzata ad una visione positiva del martirio per una causa, perché quel comportamento esca da un'area lecita e si immerga nel mare della sanzione penale.

---

[51] Vedi F. v. LISZT, *Der Zweckgedanke im Strafrecht*, vol. III, 1883 (trad. it. *La teoria dello scopo nel diritto penale*, Milano, 1962, in specie 46).

[52] Nello stesso senso cfr. M. PELISSERO, *Contrasto al terrorismo*, cit., 99 ss.

[53] Simile espressione evoca quelle già note di C. ROXIN, *Sinn und Grenzen staatlicher Strafe*, in *JS*, 1966, 381 e ss.; F. BRICOLA, *Tecniche di tutela penale e tecniche alternative di tutela*, in M. DE ACUTIS, G. PALOMBARINI (cur.), *Funzioni e limiti del diritto penale*, Padova, 1984, 3 ss. Cfr. F. PALAZZO, *Principi costituzionali, beni giuridici e scelte di criminalizzazione*, in *Studi in memoria di Pietro Nuvolone*, I, Milano, 1991, 369 ss.; M. DONINI, *Le tecniche di degradazione fra sussidiarietà e non punibilità*, in *Ind. pen.*, 2003, 82-83 (ora in M. DONINI, *Alla ricerca di un disegno*, Padova, 2003, 377 ss.).

Allo stesso modo fornire istruzioni per la realizzazione di un ordigno esplosivo non dovrebbe integrare di per sé comportamenti idonei a porre in essere, ad esempio, i reati di auto o etero addestramento[54].

Dovrebbe essere necessaria, dunque, la sussistenza di ulteriori elementi oggettivi ossia, ad esempio, la prova di concrete attività preparatorie di atti terroristici, oppure della creazione di una struttura criminale idonea a mettere in opera gli atti terroristici[55].

Tentando di concludere e al contempo di riassumere, nel contrasto al cyber-terrorismo non sembra indispensabile adottare, oggi, una fattispecie penale specifica, diversa ed ulteriore rispetto a quelle già applicabili nell'ambito dei settori "criminalità informatica" e "legislazione anti terrorismo". Essa rischierebbe di erigersi a paladina nella lotta di una sorta di "meta-terrorismo"[56], che potrebbe tradursi nell'usare, replicare, amplificare il potere comunicativo e diffusivo delle tecnologie utilizzate dal terrorismo per instillare la paura del terrorismo.

Il nostro legislatore sembra già affannato da scelte simboliche di anticipazione ed ampliamento della tutela dettate dall'emergenza e non sempre attente alle peculiarità del contesto tecnologico, sconfinando nella demonizzazione di Internet e degli strumenti informatici.

È pur vero che appare necessario attendere gli sviluppi della prassi applicativa per verificare se la giurisprudenza sarà in grado di svolgere un ruolo effettivo di garanzia. È altrettanto vero che affidare alla magistratura troppe risposte ne segna inevitabilmente il destino di sovraesposizione istituzionale, funzionale all'assenza di scelte da parte del potere legislativo[57].

La questione riguarda le scelte politico-criminali, le quali dimostrano timore davanti ad un universo tecnologico per la maggior parte ancora di difficile comprensione da parte del legislatore, dell'interprete e del giurista. Ne sono immediata dimostrazione le circostanze aggravanti che prevedono un aumento di pena se il fatto è realizzato attraverso strumenti informatici o telematici.

---

[54] Cfr. Cass., sez. I pen., 6 novembre 2013, n. 4433.

[55] Cfr. Cass. sez. V pen., 14 luglio 2016, n. 48001.

[56] Cfr. F. STRAZZARI, *Fra meta terrorismo e sicurezza algoritmica*, in *Quaderni e Giustizia* (speciali), 2016, 91 ss.

[57] Vedi M. DONINI, *Terrorismo*, cit., 143.

Ha ragione chi afferma che la

> scienza penale […] è fatta da diversi attori che usano oggi molti linguaggi, tra i quali ci sono anche la dogmatica classica e quella moderna, ma sempre più forti sono gli apporti della comparazione e di saperi extragiuridici[58].

In questo contesto proprio il sapere extra-giuridico svolge un ruolo fondamentale.

La scienza e il sapere tecnologico dovrebbero influenzare il diritto, in un'ottica di interazione reciproca per la comprensione dei diversi linguaggi. Oggi è proprio la complessità dei linguaggi tecnico-scientifici a mettere il legislatore ed il giudice in una condizione di inferiorità cognitiva, che nel peggiore dei casi si traduce in un approccio casistico culturalmente arretrato rispetto al livello di progresso tecnologico raggiunto.

È condivisibile la conclusione a cui giunge una parte della dottrina nell'affrontare, più in generale, il problema dei rapporti tra scienza e diritto e delle controversie tecnico-scientifiche nel diritto e nel processo penale, ossia che si tratti di un «paradosso al quale oggi non ci si può sottrarre». Si tratta di «saperlo gestire, guardandosi dal duplice pericolo che la scienza espropri il diritto, e che il diritto ignori o rinneghi la scienza. Impresa realizzabile in linea di astratto principio, ma difficile nei fatti»[59].

Un più efficace contrasto al fenomeno cyber-terrorismo necessita del superamento di tale difficoltà.

Si tratta ora di impostare l'opera ermeneutica su modelli interpretativi basati sull'interazione reciproca fra regola giuridica e regola tecnologica. Solo grazie all'esperienza applicativa anche il legislatore potrà avere gli strumenti per verificare l'effettività delle norme incriminatrici attualmente in vigore e, eventualmente, l'esigenza di introdurre disposizioni *ad hoc*, in cui l'elemento tecnologico svolga un "ruolo" nella

[58] M. DONINI, *Tecnicismo giuridico e scienza penale cent'anni dopo. La prolusione di Arturo Rocco (1910) nell'età dell'europeismo giudiziario*, in *Criminalia*, 2010, 178.

[59] G. FIANDACA, *Il giudice di fronte alle controversie tecnico-scientifiche. Il diritto e il processo penale*, in *D.&Q. pubb.*, 2005, 22-23.

struttura della fattispecie, ma non per la sua natura e le sue potenzialità, bensì per le modalità di utilizzo da parte del reo, con la consapevolezza che il "significato" di una tecnologia dipende dall'uso che se ne fa, esattamente come il significato di una parola dipende dall'uso della parola[60].

[60] L'espressione trae spunto dalla «tecnologia pragmatica» di John Dewey: vedi L.A. HICKMAN, *John Dewey's Pragmatic Technology*, Indiana University Press, Bloomington, 1990. A parere dell'Autore, Dewey è il filosofo della «tecnologia pragmatica», perché tutta la sua opera è attraversata direttamente o indirettamente dal concetto di «tecnologia», il cui ruolo centrale è stato analizzato molto prima rispetto alle due figure dominanti del tardo ventesimo secolo, ossia Jacques Ellul e Martin Heidegger.

# IL DIRITTO PENALE DEI *SOFTWARE* "A DUPLICE USO"

*Ivan Salvadori*



## *1. Introduzione*

Negli ultimi decenni, in conseguenza dell'incessante sviluppo tecnologico, sono notevolmente aumentate le possibilità di aggredire non solo beni giuridici tradizionali (patrimonio, onore e reputazione, proprietà intellettuale, libertà di autodeterminazione in ambito sessuale, ecc.), ma anche interessi meritevoli e "bisognosi" di tutela penale del tutto nuovi, come la riservatezza informatica, l'integrità e la disponibili-

tà di dati e di sistemi informatici[1]. Si è così assistito ad un considerevole incremento dei reati informatici ed in specie dei reati cibernetici (*cyber crimes*), commessi mediante le reti telematiche e Internet[2].

Di regola, la commissione di tali reati non richiede elevate conoscenze informatiche. Per ledere la reputazione di una persona per mezzo del *web* basta pubblicare un messaggio diffamatorio su un *blog* o su un *Social Network*[3]. Lo stesso dicasi per i sempre più frequenti casi di adescamento di minori per scopi sessuali (*child-grooming*) ovvero di diffusione e cessione di immagini pedopornografiche in rete (*sexting*, *revenge porn*, ecc.). Per commettere tali reati cibernetici "in senso ampio" è sufficiente disporre di un sistema informatico e di una buona connessione ad Internet.

Maggiori competenze informatiche sono necessarie invece per poter accedere abusivamente a *computer* protetti da misure di sicurezza (*hacking* o *cracking*), per intercettare fraudolentemente i dati informati-

[1] Sull'emersione e la dimensione sociale di questi nuovi beni giuridici nella società dell'informazione v. già L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21 ss., 70 ss.; più di recente I. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in L. PICOTTI (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 125 ss., 149 ss.

[2] Sulla rilevanza penale delle nuove minacce commesse sul *web* sia consentito rinviare, rispetto al nostro ordinamento giuridico, a I. SALVADORI, Hackg*,* cracking *e nuove forme di attacco ai sistemi di informazione. Profili di diritto penale e prospettive* de jure condendo, in *Cyberspazio e diritto*, n. 3/2008, 329 ss.; in quello tedesco U. SIEBER, *Gutachten C zum 69. Deutschen Juristentag*, München, 2012, C 18-C 25; in prospettiva sovranazionale M. GERCKE, *Understanding Cybercrime, Phenomena, Challenges and Legal Responses*, settembre, 2012, disponibile al sito *http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcrimeE.pdf* (ultima consultazione: 20 febbraio 2017); UNITED NATION, *Comprehensive Study on Cybercrime*, febbraio 2013, disponibile al sito *https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf* (ultima consultazione: 20 febbraio 2017).

[3] Sui profili di responsabilità penale del *blogger* e del direttore del periodico *online* sul quale tali messaggi diffamatori vengono pubblicati, anche per un'analisi critica dei diversi orientamenti giurisprudenziali, v. I. SALVADORI, *La normativa penale sulla stampa non si applica,* de jure condito*, ai giornali telematici*, in *Cass. pen.*, n. 9, 2011, 108 ss.

ci inviati o ricevuti da un sistema informatico (*data-espionage*), per commettere subdole forme di truffa mediante *email* (c.d. *scam*) o tecniche di ingegneria sociale (*phishing*, *pharming*, *smishing*, ecc.), per creare reti *Botnet* ovvero per ostacolare o impedire il corretto funzionamento di *Server* di istituzioni pubbliche o imprese multinazionali (*DoS* o *DDS attacks*, ecc.). La commissione di questi sofisticati comportamenti illeciti richiede la disponibilità ed il corretto utilizzo di *software* "malevoli" (c.d. *malware*)[4].

Molti di questi insidiosi programmi informatici sono facilmente reperibili in rete e soprattutto nel c.d. *Deep-web*. In questo ambito oscuro della rete si trova un fiorente mercato nero "virtuale", tramite il quale è possibile procurarsi ogni tipo di oggetto illecito (sostanze stupefacenti, materiale pedopornografico, armi, passaporti falsi, carte di credito clonate, ecc.), nonché molteplici tipologie di *malware*[5].

La maggior parte dei suddetti *software* possono essere scaricati gratuitamente dal *web*, in modo pressoché anonimo (utilizzando, ad es., un *browser* come TOR). Di contro, quelli più sofisticati e pericolosi sono, di regola, molto costosi o possono essere presi a noleggio anche solo per alcune ore. Chi ne ottiene la disponibilità, può compiere gravi e ripetuti atti illeciti con pochi *click* del *mouse*. Si tratta invero di programmi che "automatizzano" la realizzazione di comportamenti criminali e permettono di sferrare attacchi "seriali" in un brevissimo lasso temporale e di colpire sistemi informatici che si trovano in qualsiasi parte del mondo (si pensi, ad es., agli *spam-toolkits* che consentono di inviare migliaia di *e-mail* in pochi minuti).

Ad utilizzare i programmi *malware* più complessi sono soprattutto *hacker* e *cracker* o vere e proprie organizzazioni criminali alla ricerca di facili profitti sul *web*, cyber-terroristi ed in alcuni casi anche gli Stati,

[4] In questa sede il concetto di *malware* verrà impiegato in senso ampio per riferirsi ai *software* che permettono di commettere illeciti penali, ed in specie di accedere abusivamente ad un sistema informatico (*hacking tools*), di danneggiare dati o sistemi informatici (*virus*, *worm*, *ransomware*, ecc.), di eludere misure tecnologiche che proteggono opere dell'ingegno (*cracking tools*) o di intercettare dati informatici (*spyware*, *trojan horses*, *key-logger*, ecc.).

[5] In argomento v. W. LACSON, B. JONES, *The 21st Century DarkNet Market: Lessons from the Fall of Silk Road*, in *IJCC*, vol. 10, Issue 1, 2016, 40 ss.

come dimostrano i recenti episodi di guerra c.d. cibernetica (*cyber warfare*) e di spionaggio politico (*cyber-espionage*)[6].

L'elevata domanda di questi *tools* ha favorito l'emergere di un fiorente mondo illegale *underground*, che ottiene ogni anno enormi guadagni dalla vendita di pericolosi dispositivi e programmi informatici. La facile reperibilità ed al contempo fruibilità di questi *software* per scopi illeciti fa sì che il numero dei c.d. *cyber criminals* sia in continuo aumento, con il serio rischio di una criminalità cibernetica di massa, difficilmente contrastabile, dato anche il suo carattere transnazionale[7].

Per far fronte alla minaccia rappresentata dai *malware*, negli ultimi anni gli organismi internazionali, tenendo conto del preoccupante aumento di questo fenomeno, confermato da studi empirici e criminologici, hanno raccomandato o prescritto agli Stati di sanzionare un ampio ventaglio di fattispecie che hanno ad oggetto un *software*, che può essere utilizzato per commettere un reato. Si tratta, di regola, di condotte "neutre", inidonee ad offendere un bene giuridico. Il disvalore sociale di queste incriminazioni va piuttosto individuato nella intrinseca pericolosità dei programmi che ne costituiscono l'oggetto materiale e che per il fatto di rientrare nella sfera di disponibilità del soggetto agente possono essere utilizzati per fini illeciti o comunque consegnati o distribuiti a soggetti malintenzionati, favorendo ed incentivando la commissione di reati cibernetici.

---

[6] Sulle nuove minacce alla pace ed alla sicurezza internazionale rappresentate dall'utilizzo illecito di c.d. "armi cibernetiche" (*cyber weapons*) nell'ambito di conflitti armati tra Stati e le nuove sfide per il diritto (penale) internazionale v., per tutti, M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014; ed in specie M.N. SCHMITT (ed.), *Tallinn Manual on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge, 2017; sulla possibilità di applicare i crimini internazionali previsti dallo Statuto di Roma agli attacchi cibernetici v., anche per essenziali riferimenti bibliografici, il contributo di K. AMBOS, *International Criminal Responsibility in Cyberspace*, in N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, 118 ss.

[7] È significativo il fatto che tra i settori di criminalità grave e transnazionale l'art. 83 TFUE richiami anche la criminalità informatica. Sul punto v. i rilievi di L. PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. econ.*, n. 4, 2011, 827 ss.

Per definire questa peculiare tipologia di norme incriminatrici nella dottrina tedesca è stata coniata l'icastica espressione di *software-Delikte*[8]. Essa rende bene l'idea di come il baricentro di queste previsioni legali poggi essenzialmente sulla pericolosità del programma informatico che costituisce l'oggetto materiale del reato.

Nel nostro ordinamento il "diritto penale dei *software*" ha fatto la sua comparsa non solo nella parte speciale del codice penale, ma anche nella legislazione complementare (v. *infra*, par. 7). Si pensi, ad esempio, alle fattispecie che puniscono i *software* destinati a violare le misure tecnologiche di protezione delle opere tutelate dal *copyright* (di seguito: TPMs), a falsificare monete, carte filigranate o altri mezzi di pagamento (carte di credito, bancomat, ecc.), ad accedere abusivamente ad un sistema informatico protetto da misure di sicurezza o a servizi radiotelevisivi criptati, ad intercettare o interrompere illecitamente comunicazioni elettroniche tra sistemi telematici, a danneggiare dati e sistemi informatici privati o "pubblici", ecc.

Mediante le incriminazioni che riguardano questi programmi informatici si previene la commissione di ulteriori reati (contro il patrimonio, la fede pubblica, la riservatezza informatica, la integrità e la disponibilità dei dati e dei sistemi informatici, ecc.). In questo modo si puniscono comportamenti prodromici o, in alcuni casi, preparatori alla commissione di più gravi reati, ostacolando la realizzazione di fatti maggiormente offensivi dei beni giuridici tutelati. Si tratta dunque di norme incriminatrici che si inseriscono nell'alveo del diritto penale c.d. preventivo: anziché punire comportamenti socialmente dannosi e offensivi di interessi giuridici, tendono a impedire e *prevenire* appunto la commissione di futuri reati[9].

---

[8] Tale felice definizione è stata impiegata per la prima volta nella dottrina germanica da A. POPP, *§ 202c StGB und der neue Typus des europäischen »Software-Delikts«*, in *GA*, 2008, 375 ss., a commento della fattispecie introdotta nel codice penale tedesco con il 41. *StrÄndG* del 7 agosto 2007, che punisce gli atti preparatori all'accesso ed all'intercettazione di dati informatici («Vorbereiten des Ausspähens und Abfangens von Daten») di cui al § 202c D-StGB.

[9] Cfr. L. PICOTTI, *Sicurezza, informatica e diritto penale*, in M. DONINI, M. PAVARINI (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, 217 ss., 221 ss. Più in generale, sulle caratteristiche del diritto penale preventivo, basti qui rinviare agli approfonditi contributi di W. WOHLERS, *Deliktstypen des Präventionsstrafrechts. Zur Dogmatik*

L'autonoma incriminazione della produzione, della messa a disposizione o del mero fatto di procurarsi o detenere un *malware* riflette un innegabile dato empirico e criminologico. La criminalità informatica ed in specie cibernetica per la sua complessità tecnica favorisce la possibilità di frazionamento dell'*iter criminis* ed il riparto di ruoli nell'esecuzione dell'attività criminosa.

Numerose indagini investigative condotte a livello europeo e transnazionale dimostrano come nel *cyberspazio* operino vere e proprie organizzazioni criminali con una distribuzione di compiti secondo le abilità informatiche di ciascun affiliato[10]. Risulta estremamente difficile per le autorità di *law enforcement* individuare gli autori dei *cyber crimes*, date le enormi possibilità di anonimato che ancora offre la rete. Per rimanere al passo con la continua evoluzione del *cybercrime* il legislatore è costretto non solo ad abbandonare il paradigma tradizionale del reato di evento, ma altresì a superare i classici requisiti richiesti per punire a titolo di tentativo e di concorso di persone del reato, per selezionare, nella variegata fenomenologia delle condotte illecite che vengono commesse in rete, quelle che assumono un oggettivo significato prodromico o preparatorio alla commissione di futuri reati o che si sostanziano in un potenziale contributo atipico di partecipazione[11]. In questo modo l'ordinamento cerca di scongiurare la realizzazione di più

---

*„moderner" Gefährdungsdelikte*, Berlin, 2000, *passim*; e W. HASSEMER, *Sicherheit durch Strafrecht*, in *ZIS*, 2006, 266 ss.; nella nostra dottrina v., anche per essenziali riferimenti alla letteratura di lingua tedesca, M. DONINI, *Sicurezza e diritto penale. La sicurezza come orizzonte totalizzante del discorso penale*, in M. DONINI, M. PAVARINI (a cura di), *Sicurezza*, cit., 11 ss., 14 ss., che sottolinea come l'esigenza di garantire una maggiore sicurezza alla collettività abbia di fatto favorito il passaggio da uno Stato di diritto ad uno Stato di prevenzione.

[10] Sulle caratteristiche delle organizzazioni criminali che operano sul *web* v. l'interessante studio criminologico di R. BROADHURST, P. GRABOSKY, M. ALAZAB, S. CHON, *Organizations and Cyber Crime: An Analysis of The Nature of Groups engaged in Cyber Crime*, in *IJCC*, vol. 8, Issue 1, 2014, 1 ss.

[11] Sulla progressiva tipizzazione in via autonoma di «segmenti comportamentali», quali reati prodromici alla commissione del reato-finale nei sistemi giuridico-penali c.d. casistici, v. le lucide osservazioni di F.C. PALAZZO, *Il tentativo: un problema ancora aperto? (Tipicità ed offesa tra passato e futuro)*, in AA.VV., *Scritti in onore di Franco Coppi*, I, Torino, 2011, 247 ss., 259.

gravi reati, permettendo al contempo alle forze di polizia di intervenire in una fase anticipata rispetto alla effettiva causazione del danno.

Le incriminazioni concernenti i programmi informatici che possono essere impiegati per scopi illeciti (*trojan horse*, *virus*, *spyware*, *hacking tools*, ecc.) e costituiscono una vera minaccia per i beni giuridici meritevoli e "bisognosi" di tutela penale (patrimonio, riservatezza o sicurezza informatica, ecc.) sollevano però notevoli questioni già sul piano della tecnica legislativa. Per evitare che la formulazione di tali norme incriminatrici diventi obsoleta nel giro di pochi anni, il legislatore deve far ricorso ad un linguaggio tecnico-informatico di ampio significato, tramite il quale non è sempre agevole individuare il comportamento concretamente incriminato ed il sottostante interesse leso o messo in pericolo. La necessità di contemperare le diverse esigenze mediante l'impiego di concetti elastici, spesso mutuati dal linguaggio del settore, si può scontrare con la contrapposta esigenza di garantire sufficiente determinatezza-tassatività al precetto. Queste frizioni derivano in particolar modo dalla difficoltà di selezionare con la dovuta precisione i *software* che sono oggettivamente pericolosi.

Molti dei programmi informatici che vengono impiegati per commettere un reato possono essere utilizzati al contempo per finalità del tutto lecite. Si pensi, a titolo esemplificativo, ad un *software* per criptare *file*. Esso permette a qualsiasi utente di proteggere con una *password* i documenti salvati sul proprio *computer* o su un supporto esterno (ad es. USB), impedendo a terzi di accedervi abusivamente e prendere conoscenza del loro contenuto. Questi *software* vengono sempre più spesso utilizzati anche da criminali informatici per rendere inaccessibili i documenti degli utenti e chiedere loro un "riscatto" perché possano riottenerne il regolare accesso (c.d. *ransomware*). Allo stesso tempo i programmi criptografici vengono impiegati da parte di terroristi per occultare i loro piani criminali ed impedire agli inquirenti di accedere ai loro documenti.

Non è facile individuare la corretta tecnica di tipizzazione da impiegare per selezionare in modo preciso i programmi informatici pericolosi che possono essere utilizzati per commettere reati. Due sono i principali inconvenienti che sorgono nell'ambito del "diritto penale dei *software*".

Se il legislatore optasse per una incriminazione troppo restrittiva, punendo i programmi *esclusivamente* destinati a commettere un reato, vi sarebbe il rischio di creare disposizioni simboliche, la cui applicazione pratica sarebbe assai scarsa, se non impossibile[12]. Come si avrà modo di vedere meglio in seguito (*infra*, par. 4), non esistono quasi mai programmi informatici che possono essere utilizzati *soltanto* per finalità illecite.

Dall'altro lato, una criminalizzazione più ampia avrebbe l'effetto di abbracciare condotte che di per sé non hanno un carattere offensivo o che comunque non sono necessariamente poste in essere per scopi illeciti[13]. Vi sarebbe dunque il rischio di punire anche comportamenti legittimi e socialmente accettati posti quotidianamente in essere dagli esperti del settore informatico per migliorare il livello di sicurezza dei *computer* e delle reti. Si finirebbe così con l'impedire al settore dell'*Information Technology* (di seguito: IT) di sviluppare nuovi programmi per simulare attacchi informatici, per controllare da remoto una rete per fini di analisi e di controllo, per testare antivirus o *firewall*, ecc.

Una indiscriminata criminalizzazione dei *software* pericolosi produrrebbe un c.d. *chilling effect*, dissuadendo le aziende e le multinazionali che operano nel settore IT dallo sviluppare *software*, dispositivi e nuove applicazioni per migliorare la sicurezza informatica e garantire nell'interesse della collettività un accesso sicuro alla rete ed agli spazi personali sul *web* (*email*, *Cloud*, *Home Banking*, *Social Network*, ecc.)[14].

## *2. Obiettivi ed ambito dell'indagine*

Due sono i principali obiettivi del presente contributo. Da un lato si tratterà di delineare le tecniche di tutela adottate a livello sovranaziona-

[12] Cfr. J. CLOUGH, *Principles of Cybercrime*, 2nd ed., Cambridge, 2015, 135.

[13] *Ibidem.*

[14] Cfr., rispetto alla formulazione del § 202c D-StGB, S. BORGES, C.-F. STUCKENBERG, C. WEGENER, *Bekämpfung der Computerkriminalität. Zum Entwurf Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität*, in *DuD*, 2007, 275 ss., 277.

le ed in particolare in quegli ordinamenti giuridici europei in cui l'incriminazione dei programmi "a duplice uso" (o *dual-use software*) non solo è più consolidata, ma ha anche ricevuto una più articolata e meditata elaborazione dogmatica. Sarà così possibile valutare se si sia effettivamente raggiunta una armonizzazione della legislazione penale in questo ambito ed i principali problemi che sono sorti a livello nazionale nel formulare le menzionate previsioni legali. In secondo luogo si individueranno i criteri sulla base dei quali valutare la legittimità dell'incriminazione di condotte concernenti programmi informatici che possono essere destinati alla commissione di reati.

Per raggiungere i menzionati obiettivi si dovrà definire preliminarmente il fenomeno dei prodotti "a duplice uso" (par. 3) e, ai fini della nostra indagine, il concetto di *software* "a duplice uso" (par. 4). Di seguito si richiameranno le iniziative sovranazionali in questo ambito (par. 5), ed in particolare quelle adottate dal Consiglio d'Europa (par. 5.1) e dall'Unione europea (par. 5.2). Al termine di questa prima parte si farà un preliminare bilancio critico delle tecniche di formulazione normativa impiegate per descrivere l'oggetto materiale dei suddetti precetti (par. 5.3). Nella seconda parte, sulla base di una indagine comparata dei sistemi giuridici a noi culturalmente più vicini (in specie Spagna e Germania), si analizzerà come le menzionate fonti sovranazionali siano state effettivamente attuate a livello nazionale (par. 6). Successivamente si passeranno in rassegna le norme incriminatrici previste nel nostro ordinamento che puniscono i comportamenti concernenti determinati programmi informatici (par. 7). L'analisi del diritto penale comparato e nazionale permetterà di individuare i riferimenti normativi sulla base dei quali verrà sviluppata, nella terza parte, l'indagine dogmatica e politico-criminale. Innanzitutto si tratterà di analizzare la struttura normativa delle fattispecie introdotte in questo ambito sotto il profilo del diverso grado di astrazione rispetto all'offesa dei beni giuridici da tutelare (par. 8), sistematizzando, in ragione del loro diverso significato criminoso, le condotte descritte e valorizzando la funzione di «tipizzazione» che assume la previsione del fine specifico che deve sorreggere tali comportamenti (parr. 8.1 e 8.2). Di seguito si individueranno i parametri sulla base dei quali valutare la legittimità della incriminazione di comportamenti prodromici o preparatori rispetto

alla commissione di più gravi reati informatici (par. 9). In conclusione si formuleranno, alla luce dei risultati emersi dall'indagine comparata, alcune proposte *de jure condendo* per una adeguata incriminazione delle condotte concernenti *software* "a duplice uso", maggiormente rispettosa dei fondamentali principi penalistici di rango costituzionale e convenzionale o comunque sovranazionale (par. 10).

## *3. Gli oggetti "a duplice uso"*

Il concetto di oggetti c.d. "a duplice uso" (*dual-use items*) ha una molteplicità di significati[15]. Nel linguaggio internazionale esso viene tradizionalmente impiegato per riferirsi a beni o prodotti utilizzabili al contempo in ambito civile e militare. In tal senso il regolamento 428/2009/CE stabilisce che per «prodotti a duplice uso» si debbano intendere i

> prodotti, inclusi i software e le tecnologie, che possono avere un utilizzo sia civile sia militare; essi comprendono tutti i beni che possono avere sia un utilizzo non esplosivo sia un qualche impiego nella fabbricazione di armi nucleari o di altri congegni esplosivi nucleari[16].

In un diverso contesto, l'espressione "duplice uso" viene utilizzata per riferirsi a materiali, prodotti, *hardware* o conoscenze che hanno una applicazione legittima, ma che possono essere impiegati allo stesso tempo per la fabbricazione illecita di armi chimiche o nucleari[17]. Si pensi, ad esempio, a determinate sostanze che vengono utilizzate nella produzione di inchiostro o di pesticidi, ma che possono servire anche per la preparazione di armi chimiche. Lo stesso dicasi per i batteri e i

[15] In tal senso v., ad es., A. WETTER, *Enforcing European Union Law on Exports of Dual-use Goods*, Oxford, 2009; J.B. TUCKER, *Introduction*, in ID. (ed.), *Innovation, Dual Use, and Security, Managing the Risks of Emerging Biological and Chemical Technologies*, Cambridge, 2012, 1 ss., 2.

[16] Art. 2, n. 1), Regolamento (CE) n. 428/2009 del Consiglio, del 5 maggio 2009, che istituisce un regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso.

[17] *Ibidem*.

virus, che hanno un ampio campo di impiego nel settore medico e della biologia. Essi vengono studiati e conservati negli ospedali e nei laboratori farmaceutici per elaborare nuovi antidoti, vaccini e farmaci. Al contempo, però, possono servire per creare armi batteriologiche o di distruzione di massa.

La pericolosità insita in questi oggetti impone una loro stringente regolamentazione a livello sovranazionale. Ma è assai complesso trovare un giusto equilibrio tra l'esigenza di garantire, da un lato, il loro impiego per finalità mediche, scientifiche o comunque socialmente accettate, e, dall'altro, di impedirne l'uso per scopi illeciti.

La problematica degli oggetti "a doppio uso" pervade oggi ogni ambito della scienza e della tecnica ed i problemi che da essa derivano possono cogliersi anche rispetto alle nuove tecnologie dell'informazione e della comunicazione (di seguito: TIC). Si pensi, a titolo emblematico, ai sopra menzionati *software* che, pur potendo essere impiegati per fini leciti, hanno in sé una potenziale carica lesiva, che li trasforma in efficaci "mezzi" di esecuzione di reati (tradizionali o del tutto nuovi).

Numerosi sono i provvedimenti legislativi adottati negli ultimi anni in seno all'Unione europea per garantire un efficace sistema di controllo delle esportazioni dei prodotti a duplice uso e permetterne un libero commercio tra gli Stati membri.

Il citato regolamento 428/2009/CE suddivide i «prodotti a duplice uso» in dieci categorie, che comprendono rispettivamente: materiali nucleari, impianti ed apparecchiature (cat. 0); materiali speciali e relative apparecchiature (cat. 1); trattamento e lavorazione di materiali (cat. 2); materiali elettronici (cat. 3); calcolatori (cat. 4); telecomunicazioni e "sicurezza dell'informazione" (cat. 5); sensori e laser (cat. 6); materiale avionico e di navigazione (cat. 7); materiale navale (cat. 8), materiale aerospaziale e di propulsione (cat. 9).

Sebbene nelle menzionate categorie si faccia espresso riferimento anche ai programmi informatici, nell'allegato al suddetto regolamento, che elenca in modo tassativo gli oggetti rientranti in ciascuna categoria, non vengono menzionati i *dual-use software*.

Se il fenomeno dei programmi informatici che possono essere utilizzati al contempo per finalità lecite ed illecite non viene contemplato

dalla regolamentazione comunitaria ed internazionale in materia, la loro disciplina sul piano penale solleva problemi di non facile soluzione.

Molti sono gli ordinamenti di *common law* e di *civil law* che negli ultimi anni hanno incriminato, in linea con quanto previsto dal Consiglio d'Europea e dall'Unione europea, condotte concernenti tali programmi. Prima, però, di procedere ad evidenziare le *tecniche di tipizzazione* normativa impiegate dai legislatori sovranazionali (par. 5) e da quelli nazionali in questo ambito (parr. 6 e 7) è opportuno definire meglio il concetto di programma informatico "a duplice uso", dal momento che è su tale oggetto che si colloca il baricentro del c.d. diritto penale dei *software*, analizzato in questa sede.

## *4. Nozione e caratteristiche dei* software *"a duplice uso"*

L'espressione *dual-use software* viene impiegata nel linguaggio tecnico per indicare i programmi informatici che hanno un intrinseco carattere pericoloso e che possono essere utilizzati allo stesso tempo per finalità lecite o illecite. I programmi riconducibili a questa categoria sono suddivisibili, a seconda delle loro caratteristiche, in due gruppi: 1) *software* multifunzionali; 2) *software* multiscopo[18].

I *software* multifunzionali si contraddistinguono per il fatto di svolgere diverse funzioni, di cui una però è esclusivamente pregiudizievole ed illegittima. In altre parole, nel programma informatico è contenuto un c.d. *payload*, vale a dire un codice che ha la funzione di cagionare un danno (a dati o sistemi informatici) o di eseguire una funzione illecita (ad es. accedere ad un *computer*, eludere o aggirare una *password*, ecc.).

Si pensi, a titolo esemplificativo, al programma *VLC Media Player*. Questo *software* multifunzione, assai diffuso in rete, è un lettore multimediale che permette agli utenti di riprodurre in modo del tutto lecito musica e video. Tra le sue numerose funzioni vi era, però, anche quella di aggirare talune misure di protezione dei DVD.

[18] Cfr. M. ALBRECHT, *Die Kriminalisierung von Dual-Use-Software*, Berlin, 2014, 18.

Per una corretta incriminazione dei *software* multifunzionali occorre preliminarmente stabilire se la loro funzione illecita prevalga su quelle lecite. Si tratta dunque di individuare i connotati tipici che permettano di selezionare con sufficiente determinatezza e precisione i programmi informatici che si caratterizzano per la loro intrinseca pericolosità e che pertanto possono assurgere ad oggetto materiale di un reato.

I *software* multiscopo si caratterizzano, di contro, per il fatto che la loro funzionalità dannosa o illegale può essere impiegata non solo per finalità illecite, ma anche per scopi del tutto leciti ed utili per la società. Si pensi, a titolo emblematico, ai c.d. *hacking tools*. Tali programmi sono impiegati da *hacker* e criminali informatici per accedere abusivamente a sistemi informatici protetti da misure di sicurezza. Allo stesso tempo, però, essi vengono utilizzati in modo lecito da sviluppatori informatici o da tecnici che lavorano nel settore IT per "testare" il livello di protezione di un *computer*, di una rete *WIFI* o di un sistema operativo. Non si tratta dunque di *software* di per sé illeciti, ma a renderli tali è la destinazione che ad essi viene data da chi di volta in volta li utilizza.

Tutti i programmi ed i sistemi informatici presentano di regola delle vulnerabilità (*security hole*) nei loro codici, algoritmi o protocolli. Queste falle possono essere sfruttate (*exploit*) da parte di criminali informatici per introdursi abusivamente nei dispositivi altrui per finalità illecite (per "sottrarre", intercettare o danneggiare dati, ecc.).

Per elevare il livello di sicurezza dei sistemi, i tecnici informatici creano e utilizzano costantemente nuovi *software* aventi la funzione di simulare un attacco non autorizzato. In questo modo possono testare il livello di protezione di un sistema o di una rete e individuarne le eventuali vulnerabilità e criticità (c.d. *penetration test*).

Le persone che operano nel settore IT ed i criminali informatici perseguono molto spesso, almeno apparentemente, le stesse finalità. Entrambi sviluppano e impiegano nuovi *hacking tools* o programmi *malware* per individuare le falle nei sistemi informatici, nei sistemi operativi (Windows, Mac OS, Linux, ecc.) o in una rete di *computer*. Ma mentre i primi ricorrono a questi *tools* per migliorare gli standard di sicurezza delle nuove tecnologie, i secondi se ne servono per scoprire le vulnerabilità e sfruttarle per finalità illecite. La stessa funzionalità pregiudizievole dei programmi multiscopo può dunque essere utilizzata sia

per realizzare legittimi test di controllo e simulazioni di attacchi non autorizzati, sia per scopi illeciti.

Molti programmi di tipo *malware* vengono quotidianamente creati da esperti informatici. Una loro generalizzata incriminazione inciderebbe sulla possibilità di elevare il livello della sicurezza informatica nell'interesse della collettività ed in funzione anche di prevenzione delle minacce che provengono dalla rete, e la cui proliferazione è agevolata dalle inevitabili vulnerabilità connaturate alle TIC.

Nel punire le condotte aventi ad oggetto programmi informatici "multiscopo" il legislatore, onde evitare, come si è detto, un c.d. *chilling effect*, dovrà dunque valorizzare necessariamente il fine che muove l'agente ad agire in quel determinato modo, selezionando quei comportamenti che sono strumentali al raggiungimento di uno scopo illecito. Ma su questo rilevante aspetto si avrà modo di tornare in seguito[19].

## *5. Gli obblighi di incriminazione dei* software *"a duplice uso" nelle fonti sovranazionali*

L'incriminazione sempre più frequente negli ultimi anni di condotte concernenti specifici programmi informatici nelle legislazioni penali nazionali si deve in gran parte all'implementazione degli obblighi di fonte sovranazionale. Molteplici sono gli strumenti internazionali che prescrivono agli Stati di punire una ampia gamma di comportamenti "connessi" con *software* pericolosi. A volte si tratta di obblighi di incriminazione così precisi e dettagliati che vengono pedissequamente trasfusi nei codici penali nazionali[20]. Non stupisce pertanto se in questo peculiare ambito del diritto penale dell'informatica vi sia stato un effettivo ed opportuno riavvicinamento delle legislazioni nazionali.

Non sempre gli organismi sovranazionali impongono agli Stati di ricorrere allo strumento penale per sanzionare tali comportamenti. Molto spesso si riconosce ai legislatori nazionali la facoltà di decidere quale tipo di sanzione (civile, amministrativa o penale) impiegare. Questo

[19] V. *infra*, parr. 9.2 e 10.

[20] Per una esemplificazione in prospettiva comparata v. *infra*, par. 6.

spiega perché in molti casi lo stesso comportamento costituisca in alcuni Paesi europei un illecito amministrativo, mentre in altri si configuri come un illecito penale.

Nei paragrafi successivi si richiameranno le più importanti fonti sovranazionali che prevedono una regolamentazione specifica per i programmi informatici "a duplice uso", prestando particolare attenzione alle iniziative adottate in seno al Consiglio d'Europa (par. 5.1) ed all'Unione europea (par. 5.2). Alla luce dei risultati che emergeranno dall'analisi delle menzionate fonti si farà un primo bilancio critico sulle tecniche di formulazione dei precetti previsti in questo ambito, con particolare attenzione ai relativi oggetti materiali (par. 5.3).

Occorre precisare, in via preliminare, che gli elementi essenziali dei precetti di fonte europea, ed in specie le locuzioni con le quali vengono selezionati gli *oggetti materiali*, verranno richiamati anche nella loro versione inglese e francese, nonché, ove opportuno, spagnola e tedesca. In questo modo sarà possibile verificare se le diversità nell'implementazione di tali obblighi di incriminazione siano da attribuire a meditate scelte politico-criminali ovvero (anche) ad imprecisioni nella traduzione dei testi legislativi.

### *5.1. Le convenzioni del Consiglio d'Europa*

Due sono gli strumenti adottati dal Consiglio d'Europa che prescrivono agli Stati membri di incriminare un fascio eterogeneo di condotte aventi ad oggetto specifici programmi informatici.

Nella Convenzione europea sulla tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato, firmata a Strasburgo il 24 gennaio 2001, si prescrive agli Stati membri di punire le condotte poste in essere *a fini commerciali* che consistono nella «fabbricazione», «produzione», «importazione», «distribuzione», «vendita», «noleggio», «possesso», «installazione», «manutenzione», «sostituzione» di *dispositivi illeciti* ovvero nel fare «promozione commerciale», «marketing» o «pubblicità» in favore dei suddetti oggetti (art. 4).

Nel concetto di «dispositivi illeciti» vengono ricompresi, in base alla definizione fornita dall'art. 2, lett. d), della citata Convenzione, anche i

> programmi per elaboratori elettronici *concepiti o adattati al fine di* («*designed or adapted to*»; «*conçu ou adapté pour*») *rendere possibile l'accesso in forma intelligibile ad uno dei servizi [ad accesso condizionato o di accesso condizionato]* senza l'autorizzazione del fornitore di servizi.

La Convenzione *Cybercrime* (di seguito: CoC), firmata a Budapest il 23 novembre 2001, e ad oggi ratificata da cinquantadue Stati[21], richiede ai legislatori nazionali di punire chi, al fine di commettere un reato informatico, «vende», «distribuisce», «mette a disposizione» o «possiede» codici di accesso, *password* ovvero *software* «principalmente concepiti o destinati alla commissione di («designed or adapted primarily for the purpose of committing», «principalement conçu ou adapté pour permettre la commission de»)» reati informatici contro la riservatezza informatica, la disponibilità e l'integrità di dati o di sistemi informatici, previsti dagli artt. da 2 a 5 CoC (art. 6).

### *5.2. Le decisioni quadro e le direttive dell'Unione europea*

Anche tra le iniziative adottate dapprima nell'ambito della Comunità europea e poi dell'Unione europea non mancano disposizioni che prevedono l'obbligo per gli Stati membri di punire o comunque sanzionare in modo efficace, proporzionato e dissuasivo condotte aventi ad oggetto programmi informatici utilizzabili per finalità illecite.

La direttiva 91/250/CE, successivamente sostituita dalla direttiva 2009/24/CE sulla tutela giuridica dei programmi per elaboratore, richiedeva agli Stati membri di adottare appropriate misure per punire le condotte aventi ad oggetto qualsiasi mezzo (incluso anche un programma informatico) «unicamente inteso a facilitare» («the sole intended purpose of which is to facilitate»; «ayant pour seul but de faciliter») la rimozione non autorizzata o l'elusione di dispositivi tecnici eventualmente applicati a protezione di un programma informatico (art. 7, para. 1, lett. c)).

[21] La lista aggiornata dei Paesi che hanno sottoscritto e ratificato la CoC è disponibile al sito *http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=cnFugcWY* (ultima consultazione: 20 febbraio 2017).

L'art. 4, lett. a), della direttiva 98/84/CE sulla tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato, anticipando quanto previsto dalla citata Convenzione del Consiglio d'Europa del 2001, prevedeva l'obbligo per gli Stati membri di adottare le misure necessarie (di natura non necessariamente penale) per vietare le condotte poste in essere *a fini commerciali* di «fabbricazione», «importazione», «distribuzione», «vendita», «noleggio», «possesso», «installazione», «manutenzione» o «sostituzione» di *dispositivi illeciti* ovvero di «impiego» di comunicazioni commerciali per promuovere tali oggetti.

Nel concetto di «dispositivi illeciti» venivano ricomprese le apparecchiature ovvero «i programmi per elaboratori elettronici concepiti o adattati al fine di» («designed or adapted to»; «conçu ou adapté pour») consentire l'accesso in forma intelligibile ad un servizio protetto (art. 2, lett. c)).

La direttiva 2001/29/UE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, prevede che gli Stati membri adottino adeguate misure contro la «fabbricazione», l'«importazione», la «distribuzione», la «vendita», il «noleggio», la «pubblicità per la vendita o il noleggio» o la «detenzione a scopi commerciali» di *attrezzature* (tra cui anche i programmi informatici), prodotti o componenti che siano «oggetto di una promozione, di una pubblicità o di una commercializzazione» con la finalità di («are promoted, advertised or marketed for the purpose of»; «font l'objet d'une promotion, d'une publicité ou d'une commercialisation, dans le but de»)» eludere efficaci misure tecnologiche ovvero «principalmente progettati, prodotti, adattati o realizzati con la finalità di («primarily designed, produced, adapted or performed for the purpose of»; «principalement conçus, produits, adaptés ou réalisés dans le but de»)» rendere possibile o facilitare l'elusione di efficaci misure tecnologiche (art. 6, n. 2, lett. a) e b)).

La scelta politico-criminale di punire determinati programmi informatici è stata ripresa dal legislatore europeo anche nell'ambito degli strumenti del terzo pilastro. Paradigmatica in tal senso è la decisione quadro 2000/383/GAI, relativa al rafforzamento della tutela per mezzo di sanzioni penali e altre sanzioni contro la falsificazione di monete in relazione all'introduzione dell'euro, che è stata di recente sostituita dal-

la direttiva 2014/62/UE. Essa prevede l'obbligo per gli Stati membri di punire il fatto di «produrre» fraudolentemente, «ricevere», «ottenere» ovvero «possedere» strumenti, oggetti, ovvero «programmi o dati informatici che sono per loro natura particolarmente atti a» («computer programs and data peculiarly adapted for»; «programmes d'ordinateur destinés par leur nature à») falsificare o alterare monete (art. 3, par. 1, lett. d))[22].

La decisione quadro 2001/413/GAI, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, prescrive agli Stati membri di punire il fatto di «produrre» fraudolentemente ovvero di «ricevere», «ottenere», «vendere» o «cedere» ad altri «programmi di computer appositamente allestiti («computer programmes peculiarly adapted for»; «logiciels spécialement adapté pour»)» per la perpetrazione della contraffazione o della falsificazione di strumenti di pagamento ai fini della loro utilizzazione fraudolenta ovvero «programmi di computer il cui scopo» («computer programmes the purpose of which»; «logiciels ayant pour») sia la commissione di una frode informatica (art. 4).

La recente direttiva 2013/40/UE, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI, prevede che siano puniti come reato, almeno nei casi che non sono di minore gravità, i fatti *intenzionali* e commessi *senza diritto* di «fabbricazione», «vendita», «approvvigionamento per l'uso», «importazione», «distribuzione» o «messa a disposizione» di un «programma per computer, destinato o modificato principalmente al fine di («a computer programme, designed or adapted primarily for the purpose of»; «un programme informatique, principalement conçu ou adapté pour permettre la»)» commettere un illecito contro la riservatezza informatica,

[22] Sebbene la versione italiana della direttiva non coincida pienamente con i testi in lingua inglese e francese, in cui si parla di programmi «adattati» o «destinati» a tale finalità, si evince comunque che il legislatore europeo ha voluto selezionare i *software* oggettivamente configurati per commettere attività illecite. E che quest'ultima interpretazione sia quella "autentica", viene confermato anche dal testo della direttiva in lingua spagnola (dove si impiega la locuzione *adaptados para*) e tedesca (*Beschaffenheit nach zur*). Su questa peculiare modalità di formulazione normativa si avrà modo di tornare in seguito (*infra*, par. 5.3.1).

l'integrità o la disponibilità di dati o di sistemi informatici di cui agli artt. da 3 a 6 (art. 7)[23].

### *5.3. Un primo bilancio critico sulle tecniche di formulazione impiegate a livello sovranazionale*

Dall'analisi delle due convenzioni del Consiglio d'Europa e delle decisioni quadro e delle direttive dell'Unione europea emerge come i programmi informatici che costituiscono l'oggetto materiale dei precetti sovranazionali possano sostanzialmente essere suddivisi, sulla base della tecnica di formulazione impiegata, in tre gruppi. Essi ricomprendono i programmi informatici: a) «(principalmente) concepiti o adattati per» commettere un reato; b) «oggetto di una promozione, di una pubblicità o di una commercializzazione con la finalità di» commettere un reato; c) «il cui scopo consiste nel commettere» un reato.

In alcuni casi le disposizioni sovranazionali che raccomandano o obbligano gli Stati a sanzionare determinati *software* richiedono che il fatto venga posto in essere *senza diritto* e con l'intenzione di utilizzarli per la commissione di un reato. La previsione, nell'economia delle menzionate disposizioni, di un "fine specifico" non incide, come si avrà modo di vedere meglio in seguito, soltanto sul versante dell'elemento soggettivo e della colpevolezza, ma viene a "tipizzare" e delimitare, già in punto di elemento oggettivo, il fatto-base[24].

Nei successivi paragrafi si procederà a descrivere brevemente queste diverse tecniche di tipizzazione normativa, mettendone in risalto le peculiarità e valutandone l'idoneità a risolvere la complessa problematica dei *dual-use software*. In specie occorre assicurare, da un lato, la rile-

[23] Il testo italiano della direttiva, nella parte in cui descrive l'oggetto materiale del precetto, non corrisponde alle versioni in lingua straniera. Esso sembrerebbe porre l'accento sull'intenzione di chi ha sviluppato o modificato quel determinato *software*. Va detto, però, che il legislatore europeo ha voluto punire il programma che è stato oggettivamente «concepito» o «adattato» da chi lo ha elaborato *per* essere impiegato per commettere un reato, come emerge dai citati testi in inglese e in francese, e confermato da quelli in spagnolo (*concebido o adaptado principalmente para cometer*) e in tedesco (*ausgelegt oder hergerichtet worden ist… zu begehen*).

[24] V. *infra*, par. 9.2.

vanza penale dei comportamenti illeciti che costituiscono offesa per i beni giuridici tutelati e garantire, dall'altro, la non punibilità dei comportamenti legittimamente posti in essere dai soggetti che operano nel settore IT per testare la vulnerabilità dei dispositivi tecnologici e migliorare la sicurezza dei *computer*, dei sistemi operativi e delle reti telematiche.

### *5.3.1.* Software *«concepiti o adattati per la commissione di» un reato*

La prima modalità di formulazione impiegata a livello sovranazionale abbraccia i programmi informatici «concepiti» (*designed*) o «adattati» (*adapted*) per la commissione di un reato[25].

Mediante questo genere di tipizzazione vengono selezionati i *software* che per volontà di coloro che li sviluppano o li adattano sono destinati alla realizzazione di un determinato reato (ad es. accesso abusivo ad un servizio condizionato: *Pay-TV*, *Pay per Review*, ecc.). Questo non significa, tuttavia, che il riscontro di tali caratteristiche debba essere determinato sulla base di elementi esclusivamente soggettivi.

La volontà di chi crea o adatta tali programmi informatici deve riflettersi oggettivamente nella loro struttura o, meglio, nel loro linguaggio di programmazione. Ne consegue che la destinazione illecita del *software* dovrà essere ricostruita sulla base della sua intrinseca configurazione, del suo "disegno" o algoritmo, delle sue concrete funzioni o del suo adattamento alla commissione di quel reato o gruppo di reati per cui è stato voluto o modificato. La caratteristica o "qualifica" di tali *software* non va dunque determinata in funzione della loro effettiva *idoneità* a cagionare quel reato, bensì muovendo dall'intenzione dei loro creatori a raggiungere quello specifico risultato, che deve riflettersi oggettivamente nella configurazione dei programmi.

Questa modalità di formulazione non ricomprende quei *software* che, pur essendo idonei a commettere un determinato reato, non sono stati concepiti o modificati dai loro sviluppatori per raggiungere tale risultato. In altre parole, i programmi informatici creati in buona fede

[25] Tale tecnica di formulazione viene impiegata, come si è visto, nella direttiva 2001/29/UE (artt. 4 e 2, lett. e)), e nella Convenzione del Consiglio d'Europa sulla tutela dei servizi ad accesso condizionato (art. 2, lett. d)).

per svolgere funzioni lecite non potrebbero essere inclusi tra quelli penalmente rilevanti, anche se rappresentano comunque una minaccia per i beni giuridici tutelati, potendo essere utilizzati al contempo per scopi illeciti.

Evidenti sono i limiti di questa modalità di formulazione normativa. Una volta stabilito che un determinato programma informatico è stato *concepito* o *adattato* per commettere un reato, chiunque ne abbia la disponibilità verrebbe penalmente perseguito, a prescindere dall'intenzione di commettere o meno un illecito penale. Si pensi, ad esempio, al tecnico informatico che si procuri un c.d. *hacking tool* per testare in modo legittimo la sicurezza di un dispositivo o di una rete aziendale (c.d. *control test*).

Per escludere la rilevanza penale delle condotte prive di disvalore sociale il ricorso a questa modalità descrittiva dovrebbe essere affiancato dalla previsione della specifica finalità di utilizzare tali programmi per scopi illeciti. In questo modo si punirebbero i comportamenti aventi ad oggetto *software* "a duplice uso" soltanto qualora siano strumentali alla commissione di un reato, garantendo al settore IT la possibilità di operare in modo lecito, senza rischi di incorrere in sanzioni penali.

Va detto, tuttavia, che il fine illecito che sorregga la condotta non sempre sarebbe decisivo per selezionare i fatti penalmente rilevanti. Anche a fronte dell'esistenza di tale nesso teleologico essa non sarebbe punibile qualora il programma non sia stato concepito o adattato dal suo sviluppatore per la commissione di un reato, ma si tratti soltanto di una funzione "secondaria". A rilevare, come si è detto, non sarebbe l'oggettiva *idoneità* criminosa del *software*, ma la corrispondenza delle sue specifiche caratteristiche con la destinazione "soggettiva" voluta e data dal suo produttore. Tale modalità di tipizzazione non appare dunque adeguata a delimitare con sufficiente precisione l'oggetto materiale delle fattispecie che puniscono i programmi informatici "a duplice uso", sovrapponendo o confondendo elementi oggettivi e soggettivi.

*5.3.1.1.* Software *«principalmente concepiti o adattati per» commettere un reato*

In alcuni casi le fonti sovranazionali prescrivono agli Stati di punire i programmi che sono «principalmente concepiti o adattati per» commettere un delitto[26]. Questa modalità di formulazione normativa si differenzia dalla precedente (*retro*, par. 5.3.1) nella parte in cui richiede che il programma informatico debba essere *principalmente* (*primarily*, *principalement*, *in erster Linie*) destinato o concepito dal suo sviluppatore o produttore per la realizzazione di attività illecite. Ne consegue che un *software* multifunzionale, per essere tipico, dovrà essere stato creato *in primo luogo* o *essenzialmente per* commettere un determinato reato o gruppo di reati (informatici)[27].

Come emerge dalla esposizione dei motivi della Convenzione *Cybercrime*, gli esperti del Consiglio d'Europa discussero a lungo sull'opportunità di incriminare soltanto i *software* concepiti o creati *esclusivamente* o *specificamente* per commettere un reato, escludendo in questo modo quelli "a duplice uso"[28]. Si ritenne, tuttavia, che tale scelta sarebbe stata troppo restrittiva ed avrebbe generato insormontabili problemi in sede processuale, date le evidenti difficoltà di dimostrare che un programma informatico è destinato *esclusivamente* ad una funzione illecita[29]. Si sarebbe così finito per creare una fattispecie simbolica di scarsa, se non impossibile, applicazione pratica.

Allo stesso tempo, però, si rifiutò l'approccio opposto, inteso ad includere nell'oggetto materiale del precetto qualsiasi *dual-use software*, anche se legalmente prodotto e distribuito per fini leciti. Come soluzione di compromesso, si decise dunque di selezionare soltanto quei programmi che oggettivamente risultassero concepiti o adattati *principalmente* per commettere un reato, ritenendosi che in questo modo si sa-

[26] Si tratta della formulazione adottata all'art. 6 CoC, all'art. 3, n. 1, lett. d), della decisione quadro 2000/383/GAI, all'art. 6, n. 2, lett. c), direttiva 2001/29/CE e, più di recente, all'art. 7 della direttiva 2013/40/UE.

[27] Cfr. M. ALBRECHT, *op. cit.*, 178, 181.

[28] Council of Europe, *Explanatory Report*, cit., par. 73.

[29] M. ALBRECHT, *op. cit.*, 182.

rebbero esclusi nella maggior parte dei casi i programmi informatici "a duplice uso". Questa scelta solleva, tuttavia, qualche perplessità.

Innanzitutto si limita eccessivamente l'ambito dell'oggetto materiale e, di conseguenza, del precetto. Un programmatore può creare, di regola, un *software* per diversi scopi. Quest'ultimo sarà, però, considerato tipico e quindi illecito soltanto qualora si dimostri che la sua funzione o destinazione principale era di commettere quello specifico reato o gruppo di reati. Allo stesso tempo un *software* non potrebbe integrare l'oggetto tipico nel caso in cui mediante la sua creazione si perseguano al contempo finalità lecite ed illecite. Lo stesso dicasi nell'ipotesi in cui uno sviluppatore crei un programma per uno scopo legittimo, ma successivamente si scopra che può essere impiegato anche in modo illecito. Se gli scopi presi di mira dall'originario creatore o produttore del *software* sono molteplici, sarà irrilevante il fatto che il suo utilizzatore lo impieghi per una finalità delittuosa, purché quest'ultima non rappresenti la sua *principale* funzione.

In definitiva la scelta di limitare la rilevanza ai programmi *principalmente* configurati o adattati per commettere una attività criminosa non ha alcun effetto pratico e non permette di limitare con la necessaria precisione l'oggetto materiale del reato.

Per evitare che gli sviluppatori di programmi informatici vengano puniti per la creazione, ad esempio, di un c.d. *penetration test software* si dovrebbe, ancora una volta, prevedere, sul piano "soggettivo", che il fatto sia punibile solo se venga posto in essere con il fine specifico di commettere un determinato reato. Ed in questo senso i redattori della Convenzione *Cybercrime* hanno stabilito che il fatto-base debba essere sorretto dall'intenzione (*with intent*) di utilizzare quel determinato programma allo scopo di commettere una c.d. *CIA offence*, vale a dire un illecito penale contro la riservatezza informatica, la integrità ovvero la disponibilità di dati o di sistemi informatici altrui[30]. In questo modo, come si legge nel rapporto esplicativo, si è voluto evitare una eccessiva espansione dell'ambito penale, che avrebbe avuto l'effetto indesiderato

[30] Council of Europe, *Explanatory Report*, cit., par. 73: «only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment».

di punire anche i *software* disponibili sul mercato e creati per scopi leciti[31].

La previsione, dal punto di vista "soggettivo", dell'intenzione che il programma sia utilizzato allo scopo (*for the purpose*) di commettere un reato, fa sì che vengano punite anche le condotte del soggetto che produce, distribuisce ovvero mette a disposizione un *software* destinato a commettere un reato, anche qualora abbia l'intenzione che sia una terza persona ad utilizzarlo per scopi illeciti[32]. Quando invece il fatto-base non sia sorretto da alcun fine illecito non sarà penalmente rilevante.

Senza approfondire per il momento il significato e la funzione dogmatica del "dolo specifico", sul quale si avrà modo di tornare in seguito, basti qui dire che la sua previsione risulta senz'altro opportuna[33]. Di fatto, esso permette di delimitare il novero delle condotte riconducibili nell'alveo del precetto, indipendentemente dalla circostanza che il programma informatico si trovi nella sfera di disponibilità dell'agente o fuoriesca dal suo potere di controllo.

Va detto, tuttavia, che la previsione del "fine specifico", così come formulato dall'art. 6 CoC e dall'art. 7 della direttiva 2013/40/UE, potrebbe far escludere la rilevanza di comportamenti non meno pericolosi. Coloro che producono o adattano i *software* per la commissione di reati non agiscono sempre con lo scopo di commettere un reato, ma semplicemente per trarre un profitto economico dalla loro successiva cessione, vendita o commercializzazione. Di conseguenza, non potrebbero essere

[31] Council of Europe, *Explanatory Report*, cit., par. 76.

[32] Analoga tecnica di tipizzazione viene impiegata dalla più recente direttiva 2013/40/UE contro gli attacchi informatici, che obbliga gli Stati membri a punire un ampio ventaglio di condotte aventi ad oggetto un *software* pericoloso purché il soggetto agisca con *l'intenzione di* (*with the purpose of*) *utilizzarlo per* commettere un accesso abusivo, una intercettazione informatica ovvero un danneggiamento di dati o di sistemi informatici (art. 7). Anche in questo caso il fine specifico sussisterà qualora sia lo stesso agente che con la sua condotta voglia commettere uno dei reati espressamente richiamati dal precetto ovvero qualora miri a quello scopo mediante la (futura) condotta di un terzo.

[33] Sulla peculiare funzione «tipizzante» del dolo specifico, che incide sulla definizione del "fatto" di reato, prima ancora che sul piano dell'imputazione soggettiva, v. *infra*, par. 9.2.

punite le condotte, comunque pericolose, che contribuiscono alla circolazione, specie in Internet, di questi insidiosi programmi informatici.

Ad identica conclusione si deve giungere nel caso in cui l'agente metta un *malware* a disposizione di un numero indeterminato di persone che intendono utilizzarlo per commettere un reato. Anche qualora il soggetto che "diffonde" tale programma per procurarsi un vantaggio patrimoniale si configuri la possibilità che terzi potrebbero utilizzarlo per scopi illeciti non si integrerebbero gli estremi del fine specifico[34]. A determinare il suo comportamento non è, infatti, l'interesse "di parte" del raggiungimento del "fine" espressamente tipizzato dalla previsione legale, vale a dire la commissione di un reato informatico. L'agente mira invero al perseguimento di un profitto, il cui ottenimento non dipende dal realizzarsi del suddetto fine specifico.

Come si è già avuto modo di evidenziare, l'art. 3, par. 1, lett. d)(i), della direttiva 2014/62/UE sulla protezione dell'euro impone agli Stati membri l'obbligo di punire i comportamenti aventi ad oggetto programmi informatici che «per loro natura sono particolarmente atti» alla contraffazione o all'alterazione di monete. È interessante sottolineare che in questo caso il legislatore europeo, anziché prevedere un fine specifico, ha richiesto che il "fatto" venga posto in essere «fraudolentemente» (*fraudulent*; *le fait frauduleux de*; *betrügerisches*)[35].

---

[34] Questo non significa, tuttavia, che il dolo specifico sia sempre incompatibile con il dolo eventuale. Sul punto v., per tutti, L. PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993, 595 ss., in specie 608 ss.

[35] Sebbene l'impiego di un simile avverbio nella descrizione di un precetto a livello europeo non sia molto frequente, esso ricorre spesso nella nostra legislazione penale. Si pensi, a titolo esemplificativo, alla fattispecie che punisce il fatto di intercettare *fraudolentemente* comunicazioni informatiche o telematiche (art. 617-*quater* c.p.). Lo stesso dicasi per l'originaria formulazione del reato di «false comunicazioni sociali» di cui all'art. 2621, co. 1, c.c., che puniva, con la reclusione da uno a cinque anni e la multa da due milioni a venti milioni, «i promotori, i soci fondatori, gli amministratori, i direttori generali, i sindaci e i liquidatori, i quali nelle relazioni, nei bilanci o in altre comunicazioni sociali, *fraudolentemente* espongono fatti non rispondenti al vero sulla costituzione o sulle condizioni economiche della società o nascondono in tutto o in parte fatti concernenti le condizioni medesime». La fattispecie incriminatrice sul "falso in bilancio" è stata successivamente modificata dall'art. 1 d.lgs. 11 aprile 2002, n. 61 e, più di recente, dall'art. 9 l. 27 marzo 2015, n. 69.

Si è sostenuto che mediante l'avverbio *fraudolentemente* il legislatore europeo abbia voluto dare rilievo «allo scopo di commettere una truffa»[36]. In forza della sua previsione espressa sarebbero dunque da considerarsi non punibili le condotte realizzate nell'ambito di coloro che operano regolarmente nel settore IT, dal momento che non agiscono con il fine di ingannare (*Täuschungsabsicht*) e tantomeno di commettere una truffa[37].

Va detto, tuttavia, che nella nostra prevalente dottrina si ritiene, in specie rispetto al citato delitto di cui all'art. 617-*quater* c.p., che tale avverbio abbia la funzione di connotare in termini di maggior disvalore la condotta tipica, senza incidere pertanto sul piano dell'elemento soggettivo[38].

Con questa tecnica di tipizzazione normativa andrebbe dunque esclusa la rilevanza penale delle condotte dei tecnici informatici che producano, si procurino o cedano i menzionati *software* multifunzionali per testare in modo legittimo la sicurezza di un sistema informatico altrui o di una rete aziendale.

### *5.3.2.* Software *«oggetto di una promozione, di una pubblicità o di una commercializzazione con la finalità di» commettere un reato*

La seconda tecnica di formulazione normativa, impiegata dal legislatore europeo all'art. 6, n. 2, lett. c), della citata direttiva 2001/29/UE in materia di diritto d'autore, si differenzia dalla precedente in modo sostanziale. A rilevare, infatti, non è la corrispondenza delle caratteristiche oggettive del *software* con l'intenzione del soggetto che lo ha

[36] M. ALBRECHT, *op. cit.*, 200.

[37] M. ALBRECHT, *op. cit.*, 201, il quale, a sostegno di tale tesi, richiama una comunicazione della Commissione europea sulla proposta relativa alla precedente decisione quadro 2001/413/GAI, poi sostituita dalla direttiva in esame, nella quale si suggeriva di prevedere la rilevanza penale delle condotte aventi ad oggetto *software* destinati a commettere una falsificazione di monete al fine di produrre ovvero modificare strumenti di pagamento.

[38] In tal senso v., ad es., G. PICA, *Diritto penale delle nuove tecnologie.* Computer's crimes *e reati telematici, Internet, banche dati e* privacy, Torino, 1999, 117; C. PECORELLA, *Sub art. 617*-quater c.p., in E. DOLCINI, G. MARINUCCI (a cura di), *Codice penale commentato*, III, IV ed., Milano, 2015, 670 ss., 673.

creato o adattato per la commissione di un reato o per agevolarne la realizzazione, ma la circostanza che venga reclamizzato o pubblicizzato come un dispositivo utile per commettere reati. In sostanza si punisce chi produce, chi distribuisce o comunque pubblicizza, promuove o mette in commercio programmi informatici destinati a commettere un reato. Non è necessario che il programma sia oggettivamente idoneo a realizzare un determinato illecito penale (ad es. elusione delle TPMs poste a protezione di un'opera dell'ingegno), ma basta che questo venga pubblicizzato come *strumento* utile per la commissione di un fatto illecito.

Evidente è l'incapacità di tale modalità descrittiva di delimitare con precisione i *software* che costituiscano una oggettiva minaccia per i beni giuridici tutelati. Anche il tecnico informatico che utilizza un c.d. *hacking tool* per testare la sicurezza di una rete potrebbe essere assoggettato alla sanzione criminale qualora esso venga pubblicizzato (sul *web* o comunque sul "mercato") come un mezzo per commettere un reato informatico. Di contro, anche se quel *software* fosse effettivamente idoneo a perpetrare un reato non sarebbe penalmente rilevante se non fosse stato pubblicizzato come tale dal suo sviluppatore o venditore.

### *5.3.3.* Software *«il cui scopo consiste nel commettere» un reato*

L'ultima modalità di formulazione normativa pone l'accento sullo «scopo» (*purpose*) del programma informatico. Essa era già stata impiegata dal legislatore europeo nella decisione quadro 2001/413/GAI, relativa alla lotta alla frode e alla falsificazione dei mezzi di pagamento (art. 4, par. 2), ed è stata di recente ripresa dalla direttiva 2014/22/UE sulla protezione dell'euro e di altre monete (v. *retro*, par. 5.2).

Lo *scopo* è un concetto che si attaglia all'agire delle persone e che descrive l'obiettivo verso il quale un soggetto dirige la sua condotta. È questa, secondo un settore della dottrina di lingua tedesca, una nozione predicabile soltanto delle condotte umane e non di oggetti, che di per sé non hanno alcuno scopo, ma possono eventualmente essere utilizzati secondo la finalità che viene loro data da chi li utilizza[39].

[39] M. ALBRECHT, *op. cit.*, 188.

Di fronte a questa ambiguità, si è sostenuto che lo "scopo" del programma potrebbe eventualmente essere determinato sulla base di dati statistici[40]. In sostanza si dovrebbero selezionare quei *software* che nella prassi vengono prevalentemente utilizzati per la commissione di un reato. Anche in questo modo rimarrebbero, però, notevoli perplessità nei confronti di questo genere di tipizzazione dell'oggetto materiale del precetto.

Innanzitutto si finirebbe con il punire anche il ridotto numero di soggetti che impiegano quel determinato programma per scopi leciti[41].

Allo stesso tempo un dispositivo particolarmente pericoloso potrebbe essere utilizzato soltanto da un gruppo molto limitato di criminali informatici e quindi non essere "statisticamente" impiegato, nella maggior parte dei casi, per scopi illeciti.

In definitiva appare più corretto ritenere che lo "scopo" del *software* non dipenda dall'utilizzo che ne fa il suo detentore, ma dalla sua oggettiva configurazione. La specifica destinazione di un programma informatico a commettere un reato deriva dal peculiare algoritmo di programmazione, la cui esecuzione gli permette di svolgere una determinata funzione delittuosa in modo *automatizzato* secondo le procedure tecniche proprie dell'informatica e quindi anche in (parziale) "sostituzione" dell'attività umana.

A fronte delle perplessità che può destare l'impiego della nozione di "scopo" rispetto ad un oggetto, va rilevato invece che tale modalità di formulazione normativa nel contesto dell'informatica, basandosi su parametri oggettivamente riscontrabili, permette di restringere il novero dei *software* penalmente rilevanti a quelli che sono di per sé *destinati* alla commissione di un reato. Se si adottasse questa tecnica di tipizzazione normativa anche gli esperti del settore IT che impiegano un *malware* atto a realizzare un c.d. *control test* andrebbero però puniti. Per escludere la rilevanza penale di tali comportamenti si dovrebbe ancora una volta prevedere, sul piano "soggettivo", la specifica finalità di commettere un reato.

[40] *Ibidem*.

[41] M. ALBRECHT, *op. cit.*, 189, nota 462.

## *6. L'incriminazione dei* software *"a duplice uso" nel diritto penale comparato*

Negli ultimi anni molti ordinamenti di *common law* e di *civil law* hanno incriminato una serie di condotte (produzione, distribuzione, vendita, messa a disposizione, ecc.) concernenti dati (codici di accesso, *password*, ecc.) e programmi informatici destinati alla commissione di un reato. Nella maggior parte dei casi si tratta di norme incriminatrici che sono state introdotte nel diritto interno per dare attuazione alle prescrizioni del Consiglio d'Europa e dell'Unione europea[42]. È questo, ad esempio, il motivo che ha spinto numerosi legislatori europei a punire, come richiesto dall'art. 3, co. 1, lett. d), della decisione quadro 2000/383/GAI, sostituita di recente dalla citata direttiva 2014/62/UE sulla tutela dell'euro, la fabbricazione, la vendita, la distribuzione, il procacciamento o il mero possesso di «programmi informatici destinati alla falsificazione o all'alterazione di monete»[43].

Non sempre gli strumenti sovranazionali, ed in specie quelli adottati dal legislatore europeo, prescrivono agli Stati di punire con una sanzione criminale i fatti che si sostanziano nel disporre a vario titolo di programmi informatici, che possono essere impiegati per la commissione

[42] Sugli obblighi sovranazionali di incriminazione in questo specifico ambito v. *retro*, par. 5.

[43] Il codice penale francese punisce, ad es., il fatto non autorizzato di fabbricare, impiegare o detenere «programmi informatici specialmente destinati» alla fabbricazione o alla protezione contro la contraffazione o la falsificazione di monete o valori (art. 442-5 CP); il codice penale italiano punisce, come si vedrà meglio in seguito (infra, par. 7.1), chi fabbrica, acquista, aliena o detiene «programmi informatici destinati esclusivamente» alla contraffazione o all'alterazione di monete (art. 461 c.p.); il codice penale lussemburghese punisce le condotte aventi ad oggetto «programmi informatici destinati» alla fabbricazione, alla falsificazione o all'alterazione di monete (art. 9, §1, CP); il § 149 StGB tedesco punisce chi produce, procura per sé o per altri, mette in vendita, conserva o consegna ad altri «programmi informatici che per loro natura sono idonei a» *falsificare* monete o valori bollati. Con il codice penale del 1995 il legislatore spagnolo, anticipando le scelte politico-criminali dell'Unione europea in questo ambito, ha previsto la rilevanza penale della fabbricazione, della ricezione, dell'ottenimento e della detenzione di programmi informatici «specificamente destinati» a falsificare monete, timbri, documenti, carte di credito, di debito o assegni di viaggio (art. 400 CP).

di un reato. In molti casi essi si limitano a richiedere l'adozione di misure efficaci, persuasive e proporzionate.

Nel dare attuazione alla direttiva 98/84/CE sulla tutela dei servizi ad accesso condizionato, che imponeva agli Stati membri di vietare nel loro territorio un ampio ventaglio di condotte aventi ad oggetto «programmi per elaboratori elettronici concepiti o adattati» per rendere possibile l'accesso ad un servizio protetto in forma intellegibile senza l'autorizzazione del prestatore del servizio, molti legislatori nazionali sono ricorsi allo strumento penale[44]. Nel descrivere l'oggetto materiale del reato, numerosi Stati membri hanno seguito pedissequamente la tecnica di formulazione impiegata dal legislatore comunitario[45].

La direttiva 91/250/CE sulla tutela dei programmi per elaboratore, successivamente sostituita dalla direttiva 2009/24/CE, richiedeva di adottare appropriate misure per sanzionare le condotte aventi ad oggetto qualsiasi dispositivo o programma «unicamente inteso a facilitare» la rimozione non autorizzata o l'elusione di dispositivi tecnici eventualmente applicati a protezione di un *software*.

Anche in questo caso molti legislatori nazionali hanno punito con una sanzione criminale le menzionate condotte, pur non essendo previsto alcun obbligo di ricorso allo strumento penale[46].

---

[44] Le condotte aventi ad oggetto i menzionati programmi informatici sono punite, ad es., in Spagna (art. 286.1, n. 1, CP), nel Regno Unito (S. 297A(1)(b) *Copyright, Designs and Patents Act* 1988; di seguito *CDPA*), in Austria (§ 10 *Zugangskontrollgesetz-ZuKG*), in Lussemburgo (art. 2, 2), l. 2 agosto 2002) e in Belgio (art. 3.1, *Loi concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel relatifs aux services de la société de l'information*, 12 maggio 2003). Il legislatore tedesco ha invece preferito ricorrere alla sanzione amministrativa (§ 5 della *Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten* (*ZKDSG*) del 19 marzo 2002).

[45] V., ad es., le scelte adottate in Spagna (art. 286.1, n. 1, CP: «programa informático […] diseñado o adaptado para hacer posible dicho acceso»), nel Regno Unito (S. 297A(1)(b) *CDPA*: «any apparatus which is designed or adapted to enable»), in Germania (§§ 5 e 2 *ZKDSG*: «Vorrichtungen, die dazu bestimmt oder entsprechend angepasst sind»), in Austria (§ 4(1) ZuGK: «Computerprogramm, das dazu bestimmt oder angepasst ist») e in Francia (Loi 2.08.2002: «tout équipement ou logiciel conçu ou adapté pour […]»).

[46] È stata questa la scelta adottata, ad es., dal legislatore italiano (art. 171-*ter*, lett. f-*bis*), l. dir. aut. e succ. mod.), francese (art. L335-3-1, II, 2 *Code de la propriété intel-*

Nel dare attuazione a tale previsione gli Stati hanno descritto l'oggetto materiale del reato utilizzando espressioni sostanzialmente identiche a quella impiegata a livello comunitario. Si pensi, a titolo esemplificativo, alla scelta operata dal legislatore spagnolo che originariamente puniva il fatto di fabbricare, importare, mettere in circolazione o possedere qualsiasi mezzo (incluso un programma informatico) «specificamente destinato» alla soppressione non autorizzata di dispositivi tecnici posti a protezione di opere dell'ingegno (art. 270, par. 3, CP sp.)[47].

Per delimitare il raggio di applicazione della disposizione incriminatrice, la dottrina maggioritaria spagnola aveva ritenuto opportuno richiedere, in via ermeneutica, che la condotta concernesse soltanto quei mezzi o *programmi informatici* la cui *unica* funzione fosse di sopprimere o neutralizzare i dispositivi tecnici posti a protezione delle opere tutelate da *copyright*[48]. Di conseguenza, si sarebbe dovuto considerare atipico il fatto di fabbricare, vendere ovvero disporre di *software* utiliz-

---

*lectuelle*), austriaco (§§ 90b, 91 *Urheberrechtsgesetz* (UrhG), svizzero (Art. 69a, lett. b), n. 3, *Bundesgesetz über das Urheberrecht und verwandte Schutzrechte*- URG), belga (Art. XI.291 § 1r, *Code de droit économique*), ed inglese (S. 296ZB *CDPA*). Il legislatore tedesco ha invece punito le condotte concernenti i menzionati programmi informatici con la sanzione amministrativa della multa (§§ 95a, Abs. 3, 111a, Abs. 1, b), *Gesetz über Urheberrecht und verwandte Schutzrechte- UrhG*).

[47] Per un commento critico alla norma in esame v. V. GOMEZ MARTÍN, *El art. 270.3 CP: breve historia de un despróposito*, in *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, 2007, n. 21, 81 ss.

[48] In tal senso v., ad es., A. JORGE BARREIRO, Sub *art. 270 CP*, in G. RODRIGUEZ MOURULLO (dir.), *Comentarios al Código penal*, Madrid, 1997, 776; J.J. GONZÁLEZ RUS, *Delitos contra el patrimonio y contra el orden socioeconómico (VIII). Delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores*, in M. COBO DEL ROSAL (coord.), *Curso de Derecho penal español*, *Parte especial*, II ed., Madrid, 2005, 569 ss., 582. *Contra* A. GONZÁLEZ GÓMEZ, *El tipo básico de los delitos contra la propiedad intelectual. De la reforma de 1987 al Código Penal de 1995*, Madrid, 1998, 204, il quale evidenziava come tale interpretazione avrebbe portato alla sostanziale inapplicabilità dell'art. 270.3 CP, dal momento che sarebbe stato sufficiente includere nel programma informatico una funzione aggiuntiva, diversa da quella di mera elusione delle misure di sicurezza, per rendere penalmente irrilevante il fatto.

zabili anche per altre finalità (ad es. per comprimere o criptare *file*, per formattare programmi, ecc.)[49].

Dal punto di vista dell'elemento soggettivo, la miglior penalistica richiedeva inoltre che le condotte tipiche, analogamente a quanto richiesto dall'art. 102, lett. c), LPI, dovessero essere poste in essere «per scopi commerciali»[50].

Con la recente legge organica 30 marzo 2015, n. 1, di riforma del codice penale del 1995[51], il legislatore spagnolo, tenendo conto delle numerose critiche mosse dalla dottrina, ha provveduto a modificare la citata fattispecie incriminatrice.

Il nuovo art. 270, par. 6, CP sp. punisce oggi, con la reclusione da 6 mesi a 3 anni, chi fabbrica, importa, mette in circolazione ovvero possiede con un fine commerciale «qualunque mezzo principalmente concepito, prodotto, adattato o realizzato per» facilitare la soppressione non autorizzata o la neutralizzazione di qualsiasi dispositivo tecnico che sia stato utilizzato per proteggere programmi per elaboratore ovvero altre opere, interpretazioni o esecuzioni protette dal diritto d'autore[52].

---

[49] F. MIRÓ LLINARES, *La protección penal de la propiedad intelectual en la sociedad de la información*, Madrid, 2003, 430; analogamente C. MARTÍNEZ-BUJÁN PÉREZ, *Derecho penal económico y de la empresa*, *Parte especial*, IV ed., Valencia, 2013, 195.

[50] F. MIRÓ LLINARES, *La protección penal*, cit., 433, secondo il quale, ai fini di stabilire se la detenzione dei menzionati mezzi fosse destinata alla messa a disposizione del pubblico, si sarebbe dovuto tener conto di criteri oggettivi, quali la qualità e quantità dei mezzi a disposizione; in senso conf. P. FARALDO CABANA, *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Valencia, 2009, 198.

[51] *Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*.

[52] Per un primo commento alla fattispecie novellata v. A. GALÁN MUÑOZ, *La reforma de los delitos contra la propiedad intelectual e industrial*, en G. QUINTERO OLIVARES (dir.), *Comentario a la reforma penal de 2015*, Navarra, 2015, 585 ss., 593 ss., in specie 596 ss., il quale critica la scelta di ampliare il novero dei programmi informatici che rientrano nell'oggetto materiale della fattispecie, ritenendo che in questo modo si punirebbero anche *software* che, oltre ad avere la funzione di "crackare" le misure volte a proteggere il *copyright*, possono essere utilizzati per altre utilità (ad es. per visualizzare o utilizzare opere originali prodotte per essere fruibili soltanto in un determinato territorio nazionale). Di conseguenza, secondo il citato A., sarebbe sufficiente aggiungere una qualsiasi funzione legittima ad un *software* di questo tipo per eludere la sanzione penale.

In conformità a quanto stabilito dall'art. 6 CoC, molti ordinamenti europei puniscono la produzione, la vendita, il procurarsi per l'utilizzo, l'importazione, la distribuzione, il rendere disponibile o, in taluni casi, anche il mero possesso di programmi informatici «principalmente concepiti o destinati» alla commissione di reati contro la riservatezza informatica, la disponibilità e la integrità di dati o di sistemi informatici. Paradigmatica, ancora una volta, è la scelta adottata dal legislatore spagnolo del 2015, che ha introdotto nel codice penale due nuove disposizioni (artt. 197-*ter*, par. 1, lett. a), e 264-*ter*, par. 1, lett. a), CP sp.) per punire condotte che hanno ad oggetto *hacking tools* o *malware* «concepiti o adattati principalmente» per commettere reati informatici[53].

Con il 35. *StrÄndG* del 22 dicembre 2003, di attuazione della decisione quadro 2001/413/GAI contro la lotta alle frodi e alla falsificazione dei mezzi di pagamento, il legislatore tedesco ha punito il fatto di chi, per realizzare una frode informatica, produce, procura per sé o per altri, mette in vendita, cede ovvero custodisce programmi informatici «il cui scopo è di commettere» («Computerprogramme, deren Zweck die Begehung einer solchen Tat ist») un reato di truffa (§ 263a, Abs. 3, D-StGB)[54].

---

[53] Anche il codice penale belga punisce, in conformità a quanto previsto dalla citata Convenzione, le condotte aventi ad oggetto dispositivi o dati informatici *principalmente concepiti o adattati* («principalement conçu ou adapté») per permettere la commissione di un reato di intercettazione informatica (art. 341-*bis*, § 2-*bis* CP), di accesso abusivo ad un sistema informatico ovvero di danneggiamento di dati o di sistemi informatici (art. 550-*bis*, § 5 CP). L'art. 323-3-1 CP fr., recentemente modificato dalla l. 18 dicembre 2013, n. 410, punisce chi, senza un motivo legittimo, o comunque per ragioni non riconducibili alla ricerca o alla sicurezza informatica, importa, offre, cede, mette a disposizione ovvero detiene un dispositivo, dati o programmi informatici destinati o specialmente adatti («conçus ou spécialement adaptés») a commettere un accesso abusivo ad un *computer* (art. 323-1 CP) o un danneggiamento informatico (artt. 323-2 e 323-3 CP). Il § 126c, Abs. 1, Z. 1, Ö-StGB punisce un ampio ventaglio di condotte concernenti un programma informatico che, per il suo speciale carattere («nach seiner besonderen Beschaffenheit»), è stato evidentemente creato o adattato per commettere reati informatici («ersichtlich zur Begehung… […] geschaffen oder adaptiert worden ist»).

[54] Tali fatti vengono puniti in modo meno grave (reclusione fino a tre anni o la multa) rispetto al reato consumato di frode informatica (*Computerbetrug*) di cui al § 263a, Abs. 1, D-StGB (reclusione fino a 5 anni o pena della multa). Identica è la tecnica di formulazione impiegata dal legislatore tedesco per dare attuazione all'art. 6 (*Misuse of*

Per escludere dall'oggetto dell'incriminazione i programmi informatici "a duplice uso", la dottrina tedesca richiede che i *software* abbiano come *scopo essenziale* (*wesentlicher Zweck*) quello di permettere la commissione di un reato di frode. Mediante una interpretazione restrittiva, vengono così ricondotti nell'alveo del precetto soltanto i programmi *specialmente* disegnati o adattati per falsificare monete (§ 149 D-StGB)[55] ovvero per realizzare una frode informatica (§ 263a, Abs. 3, D-StGB)[56]. Vengono invece esclusi i *software* che per la loro configurazione oggettiva sono destinati a finalità lecite, ma che possono essere utilizzati anche in modo illecito[57].

---

*Device*) della Convenzione *Cybercrime*. Il delitto di «preparazione di spionaggio o di intercettazione di dati informatici» («Vorbereiten des Ausspähens und Abfangens von Daten») di cui al § 202c D-StGB, punisce chi, per preparare un delitto di spionaggio (§ 202a D-StGB) o di intercettazione di dati (§ 202b D-StGB), produce, procura per sé o per altri, acquista, cede a terzi, distribuisce ovvero mette a disposizione *password* o codici di accesso che permettono l'accesso a dati ovvero programmi informatici il cui scopo è quello di commettere uno dei menzionati reati («deren Zweck die Begehung einer solchen Tat ist»). Per un commento critico alla fattispecie in esame v. A. POPP, *§ 202c StGB*, cit., 375 ss.; E. HILGENDORF, B. VALERIUS, *Computer-und Internetstrafrecht*, 2. Aufl., Berlin-Heidelberg, 2012, 171 ss.; J. EISELE, *Computer- und Medienstrafrecht*, München, 2013, 47 ss.

[55] Il § 149 D-StGB punisce le condotte aventi ad oggetto programmi informatici che «per loro natura sono idonei a» falsificare monete o valori bollati. Secondo la dottrina maggioritaria tedesca tali programmi devono caratterizzarsi per la loro *idoneità* a falsificare o alterare monete. In tal senso v., ad es., V. ERB, *§ 149 StGB*, in W. JOECKS, K. MIEBACH (Hrsg.), *MüKo*, Bd. 2/2, §§ 80-184f StGB, München, 2005, Rn. 3, 809; analogamente T. FISCHER, *§ 149 StGB*, cit., Rn. 3, 1070, secondo cui almeno una parte del *software* deve essere utilizzabile esclusivamente per la falsificazione di denaro o di valori bollati.

[56] V. T. FISCHER, *§ 263a StGB*, cit., Rn. 32, 1925, il quale riconduce nell'oggetto materiale della fattispecie incriminatrice i *software* atti a "crackare" o decriptare *password*, programmi di tipo *spyware* o specificamente destinati a intercettare i numeri di carte di credito contenuti nelle *email*, per decodificare i servizi *Pay-TV*, ecc.; analogamente K. TIEDEMANN, B. VALERIUS, *§ 263a StGB*, in H.W. LAUFHÜTTE, R. RISSING-VAN SAAN, K. TIEDEMANN (Hrsg.), *Strafgesetzbuch*, *LK*, Bd. 9/Teil 1, 12 Aufl., Berlin, 2012, Rn. 83, 391.

[57] Di questo parere, ad es., K. CORNELIUS, *Zur Strafbarkeit des Anbietens von Hackertools*, in *CR*, 2007, 682 ss., 687; E. HILGENDORF, B. VALERIUS, *Computer- und Internetstrafrecht*, cit., Rn. 530, 158.

Un settore della dottrina germanica ha sottolineato come di fatto non esistano programmi che di per sé abbiano lo "scopo" oggettivo di commettere un reato[58]. Al riguardo viene fatto l'esempio di un programma per eludere ("crackare") le *password*, che può essere impiegato da un soggetto per recuperare la parola chiave che ha posto a protezione del suo sistema informatico, ma che ha dimenticato. In questo caso non si configurerebbe un fatto penalmente rilevante, mancando, sul piano soggettivo, l'intenzione dell'agente di servirsi del programma come mezzo per commettere una frode informatica[59].

Non vi è dubbio che per la sua idoneità intrinseca il menzionato *software* possa essere utilizzato per la commissione di una frode informatica. Ma se si seguisse questo criterio (meramente) oggettivo, nella fattispecie incriminatrice si dovrebbero sussumere anche i programmi che sono utilizzabili al contempo per finalità lecite[60].

Per restringere l'ambito di applicazione del fatto tipico, un settore della dottrina richiede che il programma debba essere stato intenzionalmente sviluppato o modificato dal soggetto che ne ha la disponibilità o dal suo sviluppatore per commettere, mediante il suo impiego, un reato[61]. Si richiede dunque la specifica destinazione (*spezifische Widmung*) del programma, da parte del suo produttore o del successivo detentore, alla commissione di un reato[62].

---

[58] A. POPP, *§ 202c StGB*, cit., 388; K. TIEDEMANN, B. VALERIUS, *§ 263a StGB*, cit., Rn. 84, 392.

[59] G. DUTTGE, *§ 263a StGB*, cit., Rn. 35, 1528.

[60] G. DUTTGE, *Vorbereitung eines Computerbetruges. Auf dem Weg zu einem "grenzlosen" Strafrecht*, in *FS-Weber*, Bielefeld, 2004, 285 ss.; dello stesso parere P. CRAMER, W. PERRON, *§ 263a StGB*, in A. SCHÖNKE, H. SCHRÖDER (Hrsg.), *Strafgesetzbuch*, 28. neu bearb. Auf., München, 2010, Rn. 33, 2388.

[61] K. CORNELIUS, *Zur Strafbarkeit*, cit., 687 s.; J. EISELE, *Payment Card Crime: Skimming*, in *CR*, 2011, 131 ss., 134.

[62] In questi termini K. CORNELIUS, *op. cit.*, 687 s., secondo cui la destinazione del programma alla commissione di un'attività illecita potrà dimostrarsi mediante il ricorso ad indizi (quali la modalità con cui viene pubblicizzato dal produttore, le istruzioni sul suo utilizzo, ecc.); analogamente S. HUSEMANN, *Die Verbesserung des strafrechtlichen Schutzes des bargeldlosen Zahlungsverkehrs durch das 35. Strafrechtsänderungsgesetz*, in *NJW*, 2004, 104 ss., 104, 108.

Il soggetto che produce o comunque dispone del menzionato *software* dovrà, di conseguenza, essere a conoscenza della sua oggettiva idoneità a realizzare un fatto costitutivo di reato.

## *7. L'incriminazione dei* software *"a duplice uso" nel diritto penale italiano*

A quanto ci consta, sette sono nel nostro ordinamento le norme incriminatrici il cui oggetto materiale è costituito da programmi informatici che possono essere impiegati per la commissione di un fatto illecito. Quattro si trovano nel codice penale e sono collocate rispettivamente tra i delitti contro la fede pubblica (art. 461 c.p.), contro la inviolabilità del domicilio (artt. 615-*quater* c.p. e 615-*quinquies* c.p.) e contro la inviolabilità dei segreti (art. 617-*quinquies* c.p.). Tre sono invece previste nell'ambito della normativa sul diritto d'autore.

Nei successivi paragrafi (7.1 e 7.2) si procederà ad analizzare, seppur nei limiti della presente indagine, i tratti essenziali delle menzionate ipotesi delittuose. Particolare attenzione verrà rivolta alla tecnica di formulazione normativa impiegata dal legislatore per descrivere l'oggetto materiale di questi reati e all'elemento soggettivo, che deve sorreggere la condotta tipica.

### *7.1. Le fattispecie previste nel codice penale*

Anticipando alcune scelte politico-criminali sovranazionali, il nostro legislatore, con la l. 23 dicembre 1993, n. 547, recante «modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica», aveva già ritenuto opportuno punire fatti che avessero ad oggetto i programmi informatici destinati a commettere determinati reati.

Con la norma incriminatrice di cui all'art. 615-*quater* c.p. («detenzione e diffusione abusiva di codice di acceso a sistemi informatici o telematici»), discutibilmente collocata nella sezione IV, concernente i delitti contro la inviolabilità del domicilio, del titolo XII del libro II del codice penale, il legislatore ha punito chi, al fine di procurare a sé o ad

altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole-chiave o altri mezzi (quali appunto programmi informatici) «idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza»[63].

La fattispecie punisce una serie di condotte prodromiche, meglio *preparatorie* alla commissione del delitto di accesso abusivo ad un sistema informatico protetto da misure di sicurezza di cui all'art. 615-*ter* c.p.[64].

Due sono le tipologie di condotte tipizzate dall'art. 615-*quater* c.p. Da un lato si puniscono i comportamenti non autorizzati che consistono nel "far entrare" nella propria sfera di signoria *password*, codice di accesso, programmi informatici ovvero altri mezzi idonei ad accedere ad un sistema informatico protetto da misure di sicurezza («si procura» o «riproduce»)[65]. Dall'altro vengono sanzionate condotte che si sostanziano nel "mettere a disposizione" di terzi tali oggetti illeciti («procura ad altri», «diffonde», «comunica» ovvero «consegna»).

Qualche perplessità sorge rispetto alla nota di "abusività" che deve caratterizzare le condotte tipiche[66]. Secondo un settore della dottrina,

---

[63] Per un primo commento critico alla menzionata fattispecie v. C. PECORELLA, *Diritto penale dell'informatica*, rist. agg., Padova, 2006, 356 ss., la quale ritiene trattarsi di un reato di pericolo (necessariamente) indiretto.

[64] Sulla struttura normativa dell'art. 615-*ter* c.p. sia consentito rinviare, anche per i necessari riferimenti bibliografici, a I. SALVADORI, *L'accesso abusivo ad un sistema*, cit., 125 ss.

[65] Diversamente da quanto previsto dalla rubrica, il precetto non contempla l'ipotesi della mera detenzione di tali dispositivi. Secondo un settore della dottrina, la detenzione andrebbe ricompresa nel fatto tipico di chi si procura i menzionati oggetti materiali. In tal senso v., ad es., G. D'AIETTI, *La tutela dei programmi e dei sistemi informatici*, in AA.VV., *Profili penali dell'informatica*, 1994, 39 ss., 81. Come si è dimostrato nell'ambito di una più ampia ricerca sui reati di possesso, il «procurarsi» (il possesso o la detenzione di) una cosa o un oggetto ricomprende ogni condotta diretta ad ottenerne la disponibilità. Si tratta pertanto di un atto che precede il possesso (o la detenzione) e che, di regola, costituisce l'*antecedente* di quest'ultimo (I. SALVADORI, *I reati di possesso*, cit., 7).

[66] Cfr. G. FIANDACA, E. MUSCO, *Dir. pen.*, *PS*, vol. II, t. I, IV ed., Bologna, 2013, 297. Analogo elemento viene richiamato nel delitto di accesso abusivo ad un sistema informatico (art. 615-*ter* c.p.). Per la sua specifica funzione nell'economia del reato ed il suo significato v., a commento di una controversa sentenza della Corte di Cassazione

mediante la previsione di tale avverbio il legislatore avrebbe voluto richiamare il giudice al suo dovere di esaminare con particolare attenzione l'assenza di cause di giustificazione[67]. Ad una prima lettura, il "fatto" di reato sarebbe, in effetti, di per sé già in grado di selezionare i comportamenti penalmente rilevanti da quelli non punibili.

A ben guardare, però, la (pur opportuna) scelta di tipizzare il "fatto", mediante la previsione di un dolo specifico, che sorregga le condotte che devono perseguire una finalità di profitto o di danno, non riesce a delimitare adeguatamente l'ambito del penalmente rilevante. Già si è detto che i tecnici che operano nel settore IT sviluppano e utilizzano regolarmente nuovi dispositivi e programmi idonei all'accesso a sistemi informatici per testarne il livello di sicurezza e l'assenza di vulnerabilità. Di regola tali programmi possono essere utilizzati dai soggetti che li producono oppure essere venduti o ceduti ad altri tecnici o *system administrator* per effettuare le necessarie verifiche sull'assenza di falle nelle TIC. Per evitare che tali condotte, di per sé legittime, vengano sussunte nell'alveo della fattispecie in esame si dovrà valorizzare la nota dell'abusività. La condotta del tecnico informatico che produce o consegna un *hacking tool* per trarne un vantaggio patrimoniale sarà «abusiva» e quindi penalmente rilevante, qualora sia contraria alle norme extrapenali che disciplinano l'attività dei soggetti che operano nel settore IT. Di contro, sarà legittima la condotta del *system administrator* che, al fine di simulare gli effetti dannosi di un attacco da parte di un *hacker*, diffonda nei sistemi di una Intranet aziendale un *Trojan*. In questo caso, pur agendo al fine di "cagionare un danno", egli non potrà essere punito, dal momento che non agisce senza autorizzazione o, me-

a sezioni unite, I. SALVADORI, *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615-ter c.p.*, in *Riv. trim. dir. pen. econ.*, 2012, n. 1-2, 369 ss., 381 ss., ed ivi riferimenti bibliografici.

[67] In questi termini v., ad es., G. MARINI, *Delitti contro la persona*, Torino, II ed., 1996, 390, che intende l'abusività come mancanza del titolo ad operare, sia per assenza del riconoscimento di tale facoltà da parte dell'ordinamento che da parte dell'avente titolo a disporne, o comunque alla presenza di scriminanti (ID., *op. cit.*, 390-391, nota p. 29); F. MANTOVANI, *Dir. pen.*, *PS*, I, V ed., Padova, 2013, 575, che ne condivide, tuttavia, la menzione espressa, in quanto richiama l'attenzione sull'illegittimità del comportamento.

glio, *abusivamente*. Con la sua condotta intende invero verificare legittimamente il livello di protezione della rete aziendale rispetto alle minacce cibernetiche.

La previsione dell'avverbio *abusivamente* arricchisce il fatto tipico qualificandolo in termini oggettivi, prima ancora che soggettivi[68]. Non si tratta dunque, come sostenuto dall'orientamento qui criticato, di constatare la mera assenza di cause di giustificazione. Mediante questa opportuna clausola di antigiuridicità speciale, il legislatore rinvia a regole extrapenali o comunque desumibili dal contesto (professionale, sociale, lavorativo, ecc.) nel quale il soggetto agente opera[69].

Per quanto riguarda la descrizione dell'oggetto materiale dell'art. 615-*quater* c.p., il legislatore ha opportunamente delimitato il novero dei programmi informatici penalmente rilevanti sulla base del criterio oggettivo della *idoneità* («mezzi idonei all'accesso») a commettere il reato di accesso abusivo ad un sistema informatico protetto da misure di sicurezza (art. 615-*ter* c.p.).

Nell'alveo della fattispecie rientrano indistintamente i programmi multifunzionali o multiscopo. L'esigenza di garantire, tuttavia, la possibilità di sviluppare programmi di contrasto agli accessi abusivi a sistemi informatici favoriti dall'impiego dei c.d. *hacking tools* viene garantita mediante l'opportuna previsione del dolo specifico, in aggiunta, come si è detto, al carattere di abusività che deve avere la condotta.

Con l'art. 4 l. n. 547/1993 cit., il legislatore ha introdotto l'art. 615-*quinquies* c.p., che punisce il delitto di «diffusione di programmi diretti a danneggiare o interrompere un sistema informatico», successivamente

[68] Il soggetto agente dovrà essere "consapevole" altresì dell'abusività della condotta, dal momento che nell'oggetto del dolo rientrano anche gli elementi normativi che concorrono a dare materia al precetto. Più in generale v. M. ROMANO, *Pre-Art. 39/63-64*, in *Commentario sistematico del Codice penale*, 3ª ed. rinn. e ampl., Milano, 2004, 324. Sulla distinzione tra clausole di illiceità espressa e speciale v., per tutti, D. PULITANÒ, *Illiceità espressa e illiceità speciale*, in *Riv. it. dir. proc. pen.*, 1967, 65 ss., 73 ss.; per una rivisitazione in prospettiva storico-comparata v. G. MORGANTE, *L'illiceità speciale nella teoria del reato*, Torino, 2002, 27 ss., 30 ss., 61 ss.

[69] Cfr. L. PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. dell'Internet*, n. 2, 2005, 189 ss., 197.

modificato, come si vedrà, nel 2008[70]. Nella sua versione originaria esso puniva, con la reclusione sino a due anni e la multa, il fatto di «diffondere», «comunicare» o «consegnare» un programma informatico «avente per scopo o per effetto» il danneggiamento di dati o di sistemi informatici.

Senza comprensibile motivo, a differenza di quanto previsto nel precedente art. 615-*quater* c.p., il legislatore puniva in questo caso soltanto le condotte volte a "far entrare" i programmi *malware* nella sfera di altri («diffonde», «comunica» ovvero «consegna»). Ma la scelta di non punire i comportamenti finalizzati a "ottenere la disponibilità" di tali programmi («si procura» o «riproduce»), più che rispondere a una meditata valutazione politico-criminale, sembrava una mera svista del legislatore[71].

L'oggetto materiale del reato era costituito dai programmi «aventi per scopo o per effetto» il danneggiamento di dati o di sistemi informatici altrui, «evento» di per sé punito autonomamente dall'art. 635-*bis* c.p.[72]. Già si è avuto modo di evidenziare come sollevi qualche perplessità, nell'ambito del c.d. diritto penale dei *software*, la scelta di limitare l'oggetto materiale del reato alla stregua dello "scopo" dei programmi informatici[73]. Ma ancor più discutibile era l'anomalo richiamo al loro «effetto» che, dovendosi intendere quale "evento" prodotto da una causa, non poteva dipendere dal concreto utilizzo che di essi fosse fatto da parte del soggetto agente. In definitiva, nell'oggetto materiale del reato venivano a cadere indistintamente tutti i *software* multifunzione e multiscopo.

A differenza di quando previsto dall'art. 615-*quater* c.p., il legislatore non aveva subordinato la rilevanza penale delle condotte al perseguimento di un fine illecito o comunque lesivo né al loro carattere

[70] Per un approfondito commento critico all'originaria formulazione della fattispecie in esame v., per tutti, C. PECORELLA, *Diritto penale dell'informatica*, cit., 235 ss.

[71] Cfr. L. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa*, *Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, n. 6, 2008, 700 ss., 708, il quale evidenzia, a ragione, come la mancata incriminazione di tali condotte contrasti con la natura di reato ostacolo dell'art. 615-*quinquies* c.p.

[72] Sul punto v. C. PECORELLA, *Diritto penale dell'informatica*, cit., 245 ss.

[73] V. *retro*, par. 5.3.3.

"abusivo", mediante la previsione di una clausola di illiceità speciale. Notevoli erano dunque le perplessità che sorgevano dal punto di vista del rispetto dei principi di determinatezza-tassatività e di offensività. Con l'impiego di questa infelice tecnica di tipizzazione normativa si punivano anche comportamenti in sé leciti e privi di disvalore sociale, come ad esempio la cessione di un *malware* da parte di uno sviluppatore informatico ad una *Software House* per testare le misure di sicurezza di un *Server* aziendale[74].

Con la l. n. 48/2008, di ratifica ed esecuzione della Convenzione *Cybercrime*, il legislatore ha finalmente modificato la criticabile formulazione della norma in esame, con il condivisibile proposito di adeguarla agli *standard* sovranazionali. L'obiettivo dichiarato di renderla «perfettamente» adeguata alle prescrizioni del Consiglio d'Europa non è stato però raggiunto.

L'opportuna estensione del novero delle condotte penalmente rilevanti anche a quelle volte a far entrare nella sfera di signoria dell'agente tali programmi («si procura», «produce», «riproduce» o «importa») ha reso la formulazione della previsione legale omogenea rispetto a quella dell'art. 615-*quater* c.p. Con l'arricchimento dell'elemento "soggettivo" di fattispecie mediante la condivisibile previsione di un dolo specifico («allo scopo di danneggiare illecitamente un sistema informatico o telematico»), il legislatore non è però riuscito, ancora una volta, a delimitare con la necessaria precisione l'oggetto materiale del reato.

Le condotte tipiche devono avere ad oggetto «apparecchiature, dispositivi o programmi informatici». Non è richiesto, però, come stabilito dall'art. 6 CoC, che questi ultimi siano «principalmente adattati o disegnati» per commettere un reato informatico contro l'integrità e la disponibilità di dati o di sistemi informatici.

Mancando ogni riferimento alla intrinseca dannosità o pericolosità dei "dispositivi" che devono essere oggetto delle condotte di per sé "neutre" di «procurarsi», «produrre», «diffondere», «distribuire» o «cedere», il disvalore della norma incriminatrice viene in modo discutibile

[74] In argomento v. già i rilievi critici di C. SARZANA, *Comunità virtuale e diritto: il problema dei Bulletin Board System*, in *Dir. pen. proc.*, 1995, 375 s.; L. PICOTTI, *La ratifica della Convenzione* Cybercrime, cit., 708-709.

a poggiare esclusivamente sul *fine illecito* che deve sorreggere il fatto-base[75]. Ma in questo modo si è tipizzata una condotta priva di offensività oggettiva. Anche chi consegna un programma informatico di per sé lecito (ad es. un sistema operativo, o un programma P2P) verrebbe ad essere punito, qualora agisse al fine di commettere un danneggiamento di dati o di sistemi informatici di cui agli artt. 615-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* c.p.[76].

Con l'art. 6 l. n. 547/1993 cit., il legislatore ha infine introdotto nel codice penale una nuova fattispecie che punisce chi, fuori dai casi consentiti dalla legge, installa apparecchiature «atte a» intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico (art. 617-*quinquies* c.p.)[77].

Nel concetto di «apparecchiature» rientrano anche i programmi informatici (*Trojan*, *Keylogger*, *Spyware*, *Sniffers*, ecc.) che, una volta installati nel sistema informatico di un utente, permettono al criminale di ottenerne l'accesso da remoto e di intercettarne le comunicazioni in entrata ed in uscita.

La delimitazione dei comportamenti penalmente illeciti in questo caso non viene determinata sulla base della previsione di una speciale finalità illecita o lesiva che debba sorreggere il fatto-base. Il *discrimen* tra comportamenti leciti ed illeciti viene invece stabilito mediante la clausola «fuori dai casi consentiti dalla legge», che il legislatore ha mutuato dalla fattispecie "gemella" dell'art. 617-*bis* c.p., già inserita nel corpo codicistico dall'art. 3 l. 8 aprile 1974, n. 98, che punisce l'instal-

[75] Cfr. L. PICOTTI, *op. cit.*, 709 s.

[76] Sulla altrettanto criticale tecnica di formulazione normativa delle fattispecie che puniscono il danneggiamento di dati e di sistemi informatici "privati" e "pubblici", che si configurano come delitti di attentato (artt. 635-*bis* e 635-*quater* c.p.) e delitti aggravati dall'evento (artt. 635-*ter* e 635-*quinquies* c.p.), sia consentito rinviare a I. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. proc. pen.*, n. 1, 2012, 204 ss.

[77] Palesemente sproporzionato (reclusione da uno a quattro anni) è il trattamento sanzionatorio previsto dalla suddetta fattispecie incriminatrice. Il fatto prodromico di installare un apparecchio atto ad intercettare o impedire una comunicazione tra sistemi informatici viene punito con la stessa sanzione criminale stabilita per chi fraudolentemente intercetta tali comunicazioni (art. 617-*quater* c.p.).

lazione di apparecchiature «atte a» intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche.

Con l'impiego di tale locuzione il legislatore aveva inteso riferirsi alle disposizioni di cui alla stessa l n. 98/1974 cit., che consideravano lecite le intercettazioni di comunicazioni telegrafiche autorizzate dall'autorità giudiziaria (artt. 5 e 6 l. cit.). Questa interpretazione dovrebbe dunque valere anche per la fattispecie in esame, introdotta nel 1993.

È evidente, tuttavia, che nell'economia dell'art. 617-*quinquies* c.p., tale clausola ha l'effetto, se interpretata letteralmente, di estendere eccessivamente l'ambito del reato, incriminando anche condotte prive di disvalore penale. Si pensi all'esigenza legittima di installare programmi di tipo *spyware* per monitorare il corretto funzionamento di una rete aziendale da parte di un c.d. *system administrator*. Meglio dunque avrebbe fatto il legislatore a prevedere, in linea con quanto previsto a livello sovranazionale, che il fatto venga commesso *senza autorizzazione* ovvero *abusivamente*.

Occorre dar conto, ai fini della presente indagine, che nel 2001, per dare attuazione alla citata decisione quadro 2000/383/GAI contro la falsificazione dell'euro, è stato esteso ai *software* l'ambito di applicazione del reato di cui all'art. 461 c.p. («fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata»), collocato fra i delitti contro la fede pubblica nel titolo VII del libro secondo del codice penale[78].

La norma incriminatrice punisce il fatto di «fabbricare», «acquistare», «detenere» o «alienare» filigrane, strumenti ovvero programmi informatici «destinati esclusivamente alla» contraffazione o alterazione di monete, di valori di bollo o di carta filigranata.

La modalità descrittiva impiegata dal legislatore per delimitare l'oggetto materiale del reato non solo si discosta da quella impiegata dall'Unione europea, che richiedeva di punire i *software* che «per loro natura sono particolarmente adattati» a falsificare monete, ma è anche eccessivamente restrittiva. Già si è detto che non esistono programmi informatici che abbiano una funzione soltanto delittuosa. Mediante que-

[78] L'art. 461 c.p. è stato così modificato dall'art. 5 d.l. n. 350/2001 cit., conv. in l. 23 novembre 2001, n. 409.

sta discutibile tecnica di formulazione normativa si è così finito con il destinare la previsione legale ad un ruolo meramente simbolico, rendendo improbabile, se non impossibile, la sua applicazione pratica.

### *7.2.* Segue: *e nella legislazione complementare*

Tre sono le norme incriminatrici previste nella legislazione in materia di diritto d'autore, che puniscono comportamenti concernenti programmi informatici. Esse sono state inserite nel nostro ordinamento dal d.lgs. 9 aprile 2003, n. 68, che ha modificato, in attuazione della citata direttiva 2001/29/CE, la l. 22 aprile 1941, n. 633, di «protezione del diritto d'autore e di altri diritti connessi al suo esercizio» e succ. mod. (di seguito: l. dir. aut.).

L'art. 171-*bis*, co. 1, l. dir. aut. punisce, con la reclusione da 6 mesi a 3 anni e la multa, chi «duplica per trarne profitto» o ai medesimi fini «importa», «distribuisce», «vende», «detiene a scopo commerciale o imprenditoriale» o «concede in locazione» qualsiasi mezzo (incluso un programma informatico) «inteso unicamente a consentire o facilitare» la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori[79].

Alquanto discutibile è la tecnica impiegata dal legislatore per delimitare l'oggetto materiale del reato. Nel linguaggio comune la voce verbale «inteso» viene riferita ad un'opera o ad una persona per indicare che tende o mira ad uno scopo[80]. Rispetto ad un oggetto, essa non denota una sua caratteristica intrinseca, ma piuttosto la destinazione che a questo viene dato da chi lo produce o eventualmente da chi lo possiede o utilizza. L'univoca funzionalità a consentire o facilitare la rimozione delle TPMs andrebbe dunque individuata sulla base di un discutibile parametro di natura soggettiva. Ma in questo modo si renderebbe incerta la sussunzione nell'oggetto materiale del delitto di cui all'art. 171-

[79] Sull'interpretazione del fine specifico di natura "commerciale" che deve sorreggere le menzionate condotte si rinvia ai condivisibili rilievi di R. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale*, Milano, 2010, 279 ss.

[80] In tal senso v. Dizionario Treccani, disponibile al sito web: *http://www.treccani.it /vocabolario/inteso1/*.

*bis*, co. 1, l. dir. aut. di un programma multifunzionale o multiscopo, che può essere utilizzato anche per violare i dispositivi che proteggono le opere tutelate dal diritto d'autore (si pensi, ad es., al già citato programma *VLC Media Player*).

E a nulla vale, per superare tali perplessità, l'aver specificato che il programma debba essere «unicamente» inteso a «consentire» o «facilitare» l'aggiramento delle misure di protezione poste a tutela di una opera dell'ingegno. Come si è detto in più occasioni, quasi mai un programma informatico svolge soltanto una funzione. Ma anche se così fosse, sarebbe molto semplice aggirare la previsione legale. Basterebbe invero programmare il *software* in modo che possa servire anche per una finalità lecita rispetto a quella che ha rilievo penale per renderlo lecito. Si tratta dunque di una tecnica di formulazione legislativa alquanto discutibile che di fatto condanna la norma incriminatrice ad un ruolo simbolico.

L'art. 171-*ter*, co. 1, lett. f), l. dir. aut. punisce, con la reclusione da 6 mesi a 3 anni e la multa, chi «introduce» nel territorio dello Stato, «detiene per la vendita o la distribuzione», «distribuisce», «vende», «concede in noleggio», «cede» a qualsiasi titolo, «promuove commercialmente», «installa» dispositivi o elementi di decodificazione speciale «che consentano» l'accesso ad un servizio criptato senza il pagamento del canone dovuto.

Il legislatore ha stabilito la rilevanza penale dei *software* che si caratterizzano per la *idoneità* («che consentano») a permettere l'accesso non autorizzato ad un servizio criptato. Anche in questo caso, però, non viene determinato con precisione il contenuto di illiceità penale del fatto di reato.

Il disvalore offensivo delle condotte, di per sé "neutre", aventi ad oggetto i programmi idonei ad accedere abusivamente ad un servizio criptato (ad es. *Pay-TV*) più che derivare dalla loro intrinseca pericolosità dipende dalla loro proiezione "commerciale"[81]. Non tutti i comportamenti tipizzati sono, però, connotati, da una dimensione patrimonialistica. Si pensi, ad esempio, alla condotta che consiste nel cedere a qualsiasi titolo (quindi anche gratuitamente) ovvero nell'installare un *soft-*

[81] Cfr. R. FLOR, *Tutela penale e autotutela tecnologica*, cit., 216 ss., in specie 219.

*ware* idoneo a decodificare un servizio a pagamento. Potrebbero astrattamente entrare nell'ambito applicativo della fattispecie in esame anche condotte aventi ad oggetto *software* idonei alla decriptazione di per sé lecite, in quanto non sorrette da alcun fine di profitto e che vengono poste in essere nell'ambito del settore IT per svolgere legittimi test sul grado di sicurezza delle TPMs apposte a suddetti servizi a pagamento.

A conclusione di questa breve rassegna, occorre infine richiamare l'art. 171-*ter*, co. 1, lett. f-*bis*), l. dir. aut. Esso sanziona, con la reclusione da 3 mesi a 3 anni e la multa, chi «fabbrica», «importa», «distribuisce», «vende», «noleggia», «cede» a qualsiasi titolo, «pubblicizza per la vendita o il noleggio», o «detiene per scopi commerciali» attrezzature, prodotti o componenti «che abbiano la prevalente finalità o l'uso commerciale» di eludere efficaci misure tecnologiche destinate a impedire o limitare atti non autorizzati dai titolari dei diritti d'autore sulle opere protette (art. 102-*quater* l. dir. aut.) ovvero «siano principalmente progettati, prodotti, adattati o realizzati con la finalità di» rendere possibile o facilitare l'elusione delle predette misure.

Notevoli perplessità solleva, anche in questo caso, la tecnica di formulazione impiegata dal legislatore, dal momento che non vengono stabiliti in modo netto i confini tra le condotte lecite e quelle illecite. La stessa descrizione degli oggetti materiali del reato non è idonea a selezionare con precisione il novero dei *software* che sono di per sé dannosi o pericolosi.

## *8. Struttura normativa e disvalore sociale dei reati il cui oggetto materiale è costituito da programmi informatici*

Dall'analisi della legislazione penale nazionale e straniera relativa al complesso fenomeno dei *software* "a duplice uso" emerge come vi sia la tendenza politico-criminale ad incriminare, in linea con le prescrizioni di fonte sovranazionale, un ampio fascio di comportamenti di diverso disvalore.

Le condotte aventi ad oggetto programmi informatici pericolosi che possono essere utilizzati per commettere un reato sono solitamente così tipizzate: «produzione», «fabbricazione», «vendita», «distribuzione»,

«messa a disposizione», «procurare per sé» o «per altri», «procurare per l'uso», «procacciamento», «acquisto», «detenzione», «detenzione per scopi commerciali», «possesso», «approvvigionamento per l'uso», «importazione», «distribuzione», «messa a disposizione in altro modo», «ricettazione», «installazione» ovvero «manutenzione a fini commerciali».

Si connotano poi per il loro peculiare carattere commerciale o comunque patrimonialistico i "fatti" che vengono incriminati nell'ambito della legislazione in materia di tutela del diritto d'autore e che hanno ad oggetto programmi informatici destinati a rimuovere o aggirare le TPMs ovvero ad accedere abusivamente a servizi criptati a pagamento. Tra questi rientrano, ad esempio, il «pubblicizzare per la vendita», il fare «noleggio», il «detenere per scopi commerciali», il «duplicare per trarne profitto», l'«importare» ai medesimi fini, il «detenere a scopo commerciale o imprenditoriale» ovvero il «concedere in locazione».

A fronte della loro equiparazione quanto ad effetti sanzionatori, si tratta di comportamenti eterogenei che presentano un diverso grado di pericolosità o di disvalore sociale a seconda dell'oggetto materiale con il quale vengono in relazione. Valorizzando, laddove espressamente previsto, anche l'elemento finalistico che deve sorreggere tali condotte, esse possono essere raggruppate sostanzialmente in due categorie.

Nella prima rientrano le condotte che consistono nell'esercizio di una *signoria* su tali *software* (par. 8.1). Nella seconda ricadono quelle che consistono nel volontario *mettere a disposizione* di terzi programmi informatici, che possono essere utilizzati per la commissione di un reato (par. 8.2).

Come ogni classificazione, anche quella qui proposta presenta dei limiti. Determinate condotte possono essere realizzate dall'agente per commettere un reato o per agevolarne la commissione a terzi. Di conseguenza, il loro inquadramento sotto l'uno o l'altro gruppo potrebbe risultare opinabile. Questo non significa, tuttavia, che la suddetta bipartizione perda la sua utilità ai fini della presente indagine. In primo luogo essa permette di cogliere non solo il diverso *grado di pericolosità* o disvalore offensivo per il bene giuridico tutelato che sta alla base di tali fatti di reato. In secondo luogo consente di individuare lo *scopo politico-criminale* che il legislatore persegue mediante la loro tipizzazione

normativa e, di conseguenza, di valutare l'opportunità della loro autonoma incriminazione.

### *8.1. La signoria su un* software *pericoloso*

Una ampia gamma di comportamenti incriminati dalle fattispecie in esame si sostanzia nell'esercizio di un controllo o di un dominio su un *software* "a duplice uso". Rientrano in questa categoria le condotte che consistono nel «fabbricare», «produrre», «acquistare», «procurarsi», «detenere», «possedere» ovvero «conservare» un programma informatico utilizzabile per commettere un reato.

Le condotte che consistono nel far entrare o nel mantenere un oggetto nella propria sfera di signoria non sempre sono sorrette dal fine specifico di commettere un reato, potendosi realizzare anche per scopi economici o commerciali. Si pensi, ad esempio, oltre alle già citate fattispecie previste dalla legislazione sul diritto d'autore (v. *retro*, par. 7.2), al delitto di detenzione e di diffusione di codici di accesso di cui all'art. 615-*quater* c.p., nella parte in cui punisce chi abusivamente «riproduce» o «si procura» codici di accesso «al fine di procurare a sé o ad altri un profitto».

Per classificare le norme incriminatrici che sanzionano queste peculiari tipologie di atti prodromici, che vanno distinti da quelli preparatori in senso stretto in quanto non sono sorretti dal fine specifico di commettere un determinato reato, un autorevole settore della dottrina tedesca ha coniato l'espressione «reati di connessione» (*Abschließungsdelikte*)[82].

In questa categoria di reati rientrerebbero le fattispecie che abbracciano condotte che di per sé non ledono né mettono concretamente in pericolo un bene giuridico, ma alle quali un terzo potrebbe "agganciarsi" con una seconda ed autonoma condotta delittuosa ed offensiva. Paradigmatici in tal senso sono i casi, tutt'altro che di scuola, in cui un soggetto tiene a disposizione di altre persone oggetti pericolosi (*mal-*

[82] U. SIEBER, *Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt. Eine Analyse der Vorfeldtatbestände im "Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten"*, in *NStZ*, H. 7, 2009, 353 ss., 358.

*ware*, armi, esplosivi, informazioni, ecc.), che potrebbero essere utilizzati da queste ultime per commettere un reato[83]. Ai fini della punibilità del c.d. "autore primario" irrilevante è che la successiva (eventuale) condotta da parte di un terzo venga effettivamente commessa[84].

Valorizzando la funzione politico-criminale, anziché la struttura normativa delle fattispecie che puniscono le condotte che si sostanziano nell'esercizio di un potere di signoria su un oggetto illecito, è possibile ricondurle alla categoria dei reati c.d. ostativi (o di ostacolo)[85].

Ponendo l'accento sulla struttura normativa di tali fattispecie esse possono essere qualificate, di regola, come reati di pericolo indiretto[86]. Si tratta in questo senso di reati che puniscono il *pericolo di un pericolo* per il bene giuridico tutelato. Si pensi, ad esempio, alle fattispecie di cui all'art. 461, co. 1, c.p. Dal fatto di «fabbricare», «acquistare» o «detenere» un programma informatico destinato alla contraffazione o all'alterazione di monete può derivare il *pericolo* di un suo (successivo) impiego per falsificare appunto le monete, con conseguente *pericolo* per l'interesse giuridico della fede pubblica e della genuinità dei mezzi di pagamento, quando siano messe in circolazione.

In determinati casi, le condotte che si sostanziano nell'esercizio di una signoria su un oggetto illecito possono essere sorrette dal *fine specifico* di commettere un determinato reato (sia da parte dell'agente che

[83] *Ibidem*.

[84] *Ibidem*.

[85] Su questa peculiare categoria di reati v., ad es., A. PAGLIARO, *Il reato*, in *Trattato di diritto penale*, *PG*, diretto da C.F. Grosso, T. Padovani e A. Pagliaro, Milano, 2007, 34; nella manualistica v. F. MANTOVANI, *Dir. pen.*, *PG*, 9ª ed., Padova, 2015, 218. Nella dottrina francese si parla al riguardo di *délits obstacles*. In tal senso v. J. PRADEL, *Droit pénal général*, 20e éd., Paris, 2014, 367 s.

[86] Sui reati di pericolo indiretto v. già V. MANZINI, *Trattato di diritto penale italiano*, I, 2ª ed., Torino, 1920, 686; F. GRISPIGNI, *Diritto penale italiano. La struttura della fattispecie legale oggettiva*, II, 2ª ed., Milano, 1952, 77; F. ANGIONI, *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983, 176 ss.; più di recente G. MARINUCCI, E. DOLCINI, *Manuale di diritto penale*, *PG*, 5ª ed., Milano, 2015, 593 ss., che distinguono tra reati di pericolo necessariamente indiretto ed eventualmente indiretto; da ultimo anche I. SALVADORI, *I reati di possesso*, cit., 234 ss.

di un terzo)[87]. È questo il caso dell'art. 615-*quinquies* c.p., che punisce chi «si procura», «produce» ovvero «riproduce» programmi informatici, di per sé non pericolosi, «allo scopo di danneggiare illecitamente un sistema informatico o telematico»[88].

Non sempre l'oggetto del "fine" che deve sorreggere la condotta è rappresentato da un reato, ma può essere anche un fatto lecito. Si pensi, a titolo esemplificativo, alla fattispecie che punisce la diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* c.p.). Di per sé lecito è il fine specifico di «procurare a sé o ad altri un profitto», non qualificato come "ingiusto".

In altri casi il fine che "muove" la condotta, pur non essendo di per sé illecito penalmente, è comunque «lesivo»[89]. Si pensi, ancora una volta, all'art. 615-*quater* c.p., nella parte in cui punisce chi abusivamente «riproduce» o «si procura» codici di accesso «al fine di arrecare ad altri un danno».

Laddove nella formulazione della norma incriminatrice il legislatore preveda espressamente che la condotta venga sorretta dalla speciale finalità di commettere un futuro reato ovvero un comportamento lesivo, le condotte incriminate acquistano un evidente carattere *preparatorio*[90]. In altre parole, il soggetto agente viene punito in quanto compie quello

[87] Si tratta dunque di reati composti di un altro reato, che costituisce l'oggetto del dolo specifico che deve sorreggere il fatto-base. Sulla peculiare categoria del "reato-elemento del reato" v. G. MORGANTE, *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale*, Torino, 2013, in specie 10 ss., 58 ss.

[88] Sulla discutibile formulazione del menzionato reato v. i rilievi critici espressi *retro*, par. 7.1.

[89] L. PICOTTI, *"Dolo specifico" und Absichtsdelikte. Der sog. Handlungszweck zwischen gesetzlicher Formulierungstechnik und dogmatischen Begriffen*, in *FS-Frisch*, Berlin, 2013, 363 ss., 376 ss.; più di recente ID., *Zwischen 'spezifischem' Vorsatz und subjektiven Unrechtselementen. Ein Beitrag zur typisierten Zielsetzung im gesetzlichen Tatbestand*, Berlin, 2014, 37 ss.

[90] Cfr. U. SIEBER, *Legitimation und Grenzen*, cit., 359, il quale, muovendo dal fondamentale ruolo che viene ad assumere "il piano delittuoso" che sorregge la condotta dell'agente, parla di *Planungsdelikte*. Su quest'ultima categoria di reati v., più di recente, U. SIEBER, B. VOGEL, *Terrorismusfinanzierung. Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht*, Berlin, 2015, 140 ss., 147 ss.

specifico "fatto" per preparare o comunque agevolare la commissione di un determinato reato.

Paradigmatiche in questo senso sono le condotte di chi «fabbrica» o «produce» un *software* al fine di commettere un reato contro la riservatezza informatica, l'integrità o la disponibilità di dati o di sistemi informatici altrui (v., ad es., artt. 197-*ter*, par. 1, lett. a), 264-*ter*, par. 1, lett. a), CP sp.)[91]. I comportamenti così tipizzati assumono un evidente significato *strumentale* alla realizzazione del reato preso di mira dal soggetto agente.

Di regola gli atti preparatori alla commissione di un reato non sono penalmente rilevanti in quanto non integrano gli elementi necessari per raggiungere la soglia del tentativo punibile[92]. Si tratta invero di comportamenti così remoti che non danno ancora inizio alla esecuzione di un reato. Essi non possono neppure considerarsi come atti «pretipici», dal momento che non sono o possono non essere ancora cronologicamente prossimi all'inizio della condotta tipica[93]. Va detto, però, che in via eccezionale il legislatore, qualora sussistano specifiche ragioni politico-criminali, può punire in via autonoma meri atti preparatori rispetto alla commissione di un più grave reato (contro l'ordine pubblico, in materia di terrorismo, ecc.)[94].

---

[91] Per un quadro generale sulla struttura dei reati informatici introdotti nel codice penale spagnolo con la riforma del 2010 sia consentito rinviare a I. SALVADORI, *I nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica 5/2010. Profili di Diritto comparato*, in *Ind. pen.*, n. 2, 2011, 767 ss., ed ivi riferimenti bibliografici. Per un primo commento critico alla successiva novella del 2015 v., limitatamente alla riformulazione dei reati informatici contro il patrimonio, P. FARALDO CABANA, *Estrategias legislativas en las reformas de los delitos informáticos contra el patrimonio*, in *Revista Aranzadi de derecho y nuevas tecnologías*, n. 26, 2016, 25 ss.

[92] Cfr., ad es., G. MARINUCCI, *Soggettivismo e oggettivismo nel diritto penale. Uno schizzo dogmatico e politico-criminale*, in *Riv. it. dir. proc. pen.*, 2011, 1 ss., 9; S. SEMINARA, *Il delitto tentato*, Milano, 2012, 834 ss.; nonché, in prospettiva comparata, L. PICOTTI, *L'élargissement des formes de préparation et de participation*, in *Rev. inter. dr. pén.*, vol. 78, 3/4 trim., 2007, 355 ss.; nella manualistica v. F. MANTOVANI, *Dir. pen.*, *PG*, cit., 434; G. MARINUCCI, E. DOLCINI, *Corso di diritto penale*, 1, 3ª ed., Milano, 2001, cit., 598 s.

[93] In tal senso F. MANTOVANI, *op. cit.*, 445.

[94] Cfr. H.-H. JESCHECK, T. WEIGEND, *Lehrbuch des Strafrechts*, *AT*, 5. voll. neubearb. u. erweit. Aufl., Berlin, 1996, 523; A. ESER, *Vorb. § 22 StGB*, in A. SCHÖNKE,

Dal punto di vista della loro struttura normativa anche i «reati preparatori» si configurano, di regola, come reati di pericolo indiretto[95]. Si pensi, a titolo esemplificativo, al fatto di chi, «al fine di arrecare ad altri un danno», si procura senza autorizzazione un *software* idoneo ad accedere abusivamente ad un sistema informatico altrui protetto da misure di sicurezza (art. 615-*quater* c.p.). Affinché il soggetto cagioni un danno ad altri, con conseguente lesione del bene giuridico dell'integrità e della disponibilità dei dati e dei sistemi informatici, occorre che si verifichi una ulteriore ed autonoma condotta (*novus actus interveniens*) di utilizzo da parte sua o di un terzo. In altre parole tra il fatto di procurarsi un c.d. *hacking tool* e l'offesa dell'interesse protetto deve esserci un passo intermedio[96]. Breve: la disponibilità di tale *malware* rappresenta il *pericolo del pericolo* di una lesione.

### *8.2. La messa a disposizione di un* software *pericoloso*

In altri casi vengono punite condotte che si sostanziano nella consapevole "messa a disposizione di terzi" di un programma informatico pericoloso. Si pensi, a titolo esemplificativo, ai fatti che consistono nel «mettere a disposizione» o anche nel «procurare ad altri» uno specifico *software*, nel «comunicare» o, meglio, nel «rendere accessibile» ovvero nel «cedere» ad un numero determinato di persone un dispositivo idoneo a commettere un reato. Il soggetto agente agevola così con la sua condotta la commissione di un reato da parte di un terzo mediante quell'oggetto, lasciando a lui la scelta se utilizzarlo per scopi illeciti.

Il «mettere a disposizione» o il «diffondere» un *malware* in rete presenta un livello di pericolosità maggiore rispetto al consegnarlo o co-

H. SCHRÖDER (Hrsg.), *Strafgesetzbuch*, cit., Rn. 13, 404-405; T. HILLENKAMP, *Vor. § 22 StGB*, in *LK*, 12. neu. bearb. Aufl., I Band, Berlin, 2007, Rn. 7, 1381.

[95] V. I. SALVADORI, *I reati di possesso*, cit., 258 ss.

[96] L'incriminazione delle condotte aventi ad oggetto *hacking tools*, che costituisce una evidente anticipazione rispetto alla consumazione materiale di un ulteriore fatto di reato più grave, è riconducibile, per la sua peculiare struttura normativa, alla categoria dei c.d. delitti a due atti incompiuti. Sui *(unvollkommene) zweiaktige Delikte* v. già K. BINDING, *Grundriss des deutschen Strafrechts*, *AT*, 6, verb. u. verm. Aufl., Leipzig, 1902, 124; nella manualistica tedesca v. H.-H. JESCHECK, T. WEIGEND, *Lehrbuch des Strafrecht*, cit., 294, nota 10.

municarlo ad un numero limitato di persone. Data la facilità con la quale è possibile duplicare o auto-eseguire i *software*, una volta che vengono immessi in rete potrebbero essere scaricati e utilizzati da un numero elevato ed indeterminato di persone e potrebbero difficilmente essere ritirati dal "mercato".

In molti casi tali condotte vengono a configurarsi come atti "preparatori" di un futuro reato commesso da un terzo, sempre che il soggetto agente sia consapevole e voglia che la persona alla quale cede o vende quel determinato *software* lo utilizzi per scopi illeciti. In sostanza l'agente agisce per aiutare un terzo a commettere un reato ovvero semplicemente per agevolarne o facilitarne la commissione. La sua condotta viene a costituire in questo caso un *contributo materiale* di natura agevolatrice alla commissione di un reato da parte di un terzo[97]. In linea con il modello dell'accessorietà minima, che il nostro legislatore ha accolto nel disciplinare l'istituto del concorso di persone del reato, l'agente, *rectius* il «partecipe» sarà punito in qualità di concorrente atipico qualora consapevolmente dia con la sua condotta un contributo causale alla realizzazione, da parti di altri, di un fatto di reato[98]. Dovrà dunque agire con il *dolo di partecipazione*, nel cui fuoco deve rientrare non solo il suo oggettivo apporto alla commissione del reato, ma anche il fatto concreto che sarà commesso dall'autore[99]. Non sarà necessario, tuttavia, che il partecipe conosca le concrete modalità di esecuzione, essendo sufficiente che si rappresenti un fatto conforme a quello tipico descritto dalla norma incriminatrice.

Non sempre le condotte che si sostanziano in una "messa a disposizione" di un *software* pericoloso integrano gli estremi di un contributo materiale ("atipico") alla realizzazione di un concreto fatto illecito commesso da altri. Di regola non sussisterà un «nesso di collegamento»

[97] Sull'agevolazione quale forma di partecipazione criminosa nel reato commesso da altri si rinvia allo studio monografico di L. STORTONI, *Agevolazione e concorso di persone nel reato*, Padova, 1981, *passim*.

[98] Sulla teoria dell'accessorietà v., per tutti, oltre al classico contributo di C. PEDRAZZI, *Il concorso di persone nel reato*, Palermo, 1952, 22 ss., in specie 28 ss.; G. INSOLERA, *Problemi di struttura del concorso di persone nel reato*, Milano, 1986, 8 ss.; S. SEMINARA, *Tecniche normative e concorso di persone nel reato*, Milano, 1987, 279 ss.

[99] G. MARINUCCI, E. DOLCINI, *Manuale di diritto penale*, *PG*, cit., 461 s.

(in tempi significativi) di natura oggettiva o soggettiva tra la condotta di chi «cede», «vende» o «distribuisce» quel determinato *malware* e il soggetto che lo utilizza per commettere un reato. In altre parole, la condotta dell'agente non sempre "accede" ad un fatto tipico altrui. Si pensi, ad esempio, ai casi in cui l'"acquirente" decida alla fine di desistere dal suo proposito criminoso e di non impiegare il *software* che ha ottenuto da altri per fini illeciti[100].

In definitiva, il legislatore tipizza in via autonoma comportamenti che acquistano un significato criminoso in quanto possono connettersi ad azioni altrui, contribuendo, *rectius* agevolandone la realizzazione. La previsione legale di queste condotte e la loro autonoma tipizzazione non ha, però, una "funzione di disciplina", ma svolge una c.d. "funzione di incriminazione". L'incriminazione, in via autonoma, delle condotte che costituiscono una volontaria "messa a disposizione" di terzi di un *software* illecito, rappresenta una deroga alla normativa sul concorso di persone nel reato, dal momento che estende la punibilità ai possibili contributi atipici, che sarebbero altrimenti impuniti[101]. Dal punto di vista politico-criminale tali fattispecie hanno dunque una funzione sostanzialmente analoga a quella dei già richiamati delitti ostativi (*retro*, par. 8.1).

[100] Non sempre l'agente è a conoscenza del fatto che il *software* che mette a disposizione di altri verrà effettivamente impiegato per commettere un reato. Si pensi, ad es., ai casi in cui un *malware* venga caricato su una pagina *web* liberamente accessibile da un numero indeterminato di utenti e dalla quale è possibile scaricarlo gratuitamente. Qualora l'agente ceda il *malware* a chi lo vuole impiegare per commettere un reato, ma quest'ultimo per diversi motivi decida di non compiere quel reato, si sarebbe di fronte ad un *tentativo di concorso*, o meglio ad un *tentativo di partecipazione* non punibile, nel nostro ordinamento, in forza dell'art. 115 c.p. Cfr., più in generale, F.C. PALAZZO, *Corso di diritto penale*, *PG*, V ed., Torino, 2013, 494 s.

[101] Colui che vende o cede a un terzo un programma *malware* sapendo che lo vuole impiegare per fini illeciti viene punito autonomamente, anche qualora quel determinato reato non si realizzi.

## *9. Sui presupposti per una legittima incriminazione dei* software *"a duplice uso"*

Dall'analisi fin qui svolta è emerso come per mezzo dell'incriminazione di comportamenti aventi ad oggetto un *software* pericoloso il legislatore anticipi la punibilità rispetto alla consumazione di un altro più grave reato, sanzionando condotte che, nel normale decorso criminoso, si collocano in una fase cronologicamente anteriore non solo rispetto alla consumazione di quel secondo reato, ma addirittura prima del suo tentativo.

Mediante questa peculiare tecnica di tipizzazione normativa si perseguono sostanzialmente due obiettivi politico-criminali. Da un lato si tratta di risolvere problemi di ordine processuale e probatorio[102]. Anticipando l'area del penalmente rilevante si permette alle autorità di *law enforcement* di svolgere indagini in un momento anteriore alla commissione di un reato più grave (di intercettazione di dati, di frode informatica, di accesso abusivo ad un sistema informatico, ecc.) e di raccogliere prove in merito a reati più complessi e difficili da accertare, nel caso di loro commissione nel *cyberspazio*[103].

In secondo luogo il legislatore persegue, almeno di regola, lo scopo di punire comportamenti che, pur non avendo ancora arrecato una lesione ad un bene giuridico protetto, ne mettono in pericolo (seppur astratto o indiretto) l'integrità. Crea dunque una barriera protettiva anticipata, in modo da ostacolare o comunque prevenire la commissione dei

[102] Ed in tal senso si potrebbe parlare, utilizzando l'icastica espressione coniata da J. Bentham, di "reati probatori": J. BENTHAM, *The Theory of Legislation*, in *Bentham's Theory of Legislation: being Principes de Législation and Traités de Législation*, trad. dal francese di Étienne Dumont (1st ed. London, 1864, rist. London, 1931, 425-427). In argomento v. anche I. SALVADORI, *I reati di possesso*, cit., 374 ss.

[103] Sulle difficoltà di svolgere indagini investigative e raccogliere prove digitali nel contesto cibernetico (c.d. *computer forensics*) v. gli interessanti contributi di R. KOSTORIS, S. MARCOLINI, M. DANIELE, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, 179-182, 190-202, 203-215; più di recente v. M. DANIELE, *Intercettazioni ed indagini informatiche*, in R. KOSTORIS (a cura di), *Manuale di procedura penale europea*, Milano, II ed. riv., 2015, 381 ss.; nella dottrina inglese v. A. STANIFORTH, *Blackstone's Handbook of Cyber Crime Investigation*, Oxford, 2015.

"fatti" che rappresentano una minaccia più grave per l'interesse tutelato.

L'incriminazione di condotte che costituiscono soltanto un pericolo indiretto per un bene giuridico non sono di per sé illegittime, ma necessitano di una forte giustificazione, dal momento che comprimono interessi fondamentali del reo (libertà personale, dignità, reputazione, ecc.), a fronte di una carica lesiva limitata. Ed in questo senso le fattispecie che hanno ad oggetto *software* pericolosi si prestano in particolar modo a fungere da banco di prova per valutare i limiti dell'anticipazione della tutela penale. È questo, infatti, un peculiare territorio del penale nel quale il legislatore fa ampio ricorso alla categoria dei c.d. «reati di prevenzione» (*Vorfeldsdelikte*), che si contrappongono ai tradizionali «reati repressivi»[104]. Vengono, infatti, puniti, comportamenti che si collocano in una fase anteriore dell'*iter criminis* che porta alla realizzazione integrale di un reato consumato, rispetto a cui o non si è verificato l'evento, o non è stata compiuta integralmente l'azione tipica. In altre parole, il legislatore punisce in via autonoma atti che, rispetto ad un'altra fattispecie incriminatrice più grave, non integrerebbero o potrebbero

[104] È questa l'espressione coniata da M. DONINI, *Modelli di illecito penale minore. Un contributo alla riforma dei reati di pericolo contro la salute pubblica*, in M. DONINI, D. CASTRONUOVO (a cura di), *La riforma dei reati contro la salute pubblica. Sicurezza del lavoro, sicurezza alimentare, sicurezza dei prodotti*, Padova, 2007, 201 ss., 254, 258-260. Va precisato, tuttavia, che l'A. citato impiega questa formula per riferirsi ai reati che si imperniano sulla inosservanza di regolamenti, regole preventivo-cautelari ovvero ordini ed obblighi. Nell'ambito della presente indagine il concetto di «reati di prevenzione» viene invece inteso in senso più lato, per riferirsi a tutte le fattispecie che si distinguono da quelle «repressive», in quanto più che punire la lesione o la messa in pericolo (astratta o concreta) di un bene giuridico incriminano comportamenti che sono prodromici o preparatori alla commissione di un reato o che comunque ne agevolano o ne facilitano la realizzazione. Ed è in questo senso che la dottrina tedesca parla di *Vorfeldsdelikte*. In argomento v. W. BECK, *Unrechtsbegründung und Vorfeldkriminalisierung. Zum Problem der Unrechtsbegründung im Bereich vorverlegter Strafbarkeit, - erörtert unter besonderer Berücksichtigung der Deliktstatbestände des politischen Strafrechts*, Berlin, 1992; U. SIEBER, *Grenzen des Strafrechts. Grundlagen und Herausforderungen des neuen strafrechtlichen Forschungsprogramms am Max-Planck-Institut für ausländisches und internationales Strafrecht*, in *ZStW*, Heft. 119, 2007, 11 ss., 27-28, che tra i settori di criminalità nei quali è sempre più frequente il ricorso ad un diritto penale preventivo richiama anche la criminalità informatica.

non integrare neppure la soglia minima del tentativo né i requisiti della partecipazione[105].

La caratteristica di questo peculiare «modello preventivo», al quale il legislatore ricorre sempre più spesso (si pensi, oltre al settore del *cybercrime*, all'ambito della lotta al terrorismo, a quelli dell'abuso e dello sfruttamento sessuale dei minori[106], della criminalità organizzata, ecc.), è che esso viene impiegato per «tutelare» o anche «creare» beni giuridici "intermedi" («"di sicurezza"»)[107]. Ma in questo modo l'intervento penale si colloca in una fase molto anteriore ed anticipata rispetto all'offesa del bene giuridico finale[108].

Come si è avuto modo di evidenziare in precedenza, nel tipizzare le condotte aventi ad oggetto *software* utilizzabili per commettere un reato o un fatto lesivo il nostro legislatore, al pari di quanto avviene in altri ordinamenti (tedesco, spagnolo, austriaco, ecc.), ricorre sostanzialmente a due tipologie di delitti[109]. Da un lato, mediante la previsione di delitti ostacolo (*délites obstacles*) vengono punite condotte che si sostanziano nell'esercizio di una signoria su un programma informatico "a duplice uso", senza però prevedere che vi sia un nesso con la futura commissione di un reato (di danneggiamento informatico, di frode, di intercettazione di dati, contro il *copyright*, ecc.). Dall'altro, mediante il ricorso alla tecnica dei *reati preparatori*, vengono sanzionate attività che servono ad agevolare, a facilitare o a "spianare" la strada verso la commissione del reato da parte dell'agente o di terzi.

Non è questa ovviamente la sede per approfondire i molteplici nodi dogmatici che solleva la complessa problematica dell'anticipazione

---

[105] In tal senso parla di reati a *consumazione* anticipata M. PARODI GIUSINO, *La condotta nei reati a tutela anticipata*, in *Ind. pen.*, 1999, 687 ss., 688.

[106] Rispetto all'anticipazione della tutela dell'integrità psico-fisica e sessuale dei minori nel diritto penale comparato sia consentito rinviare a I. SALVADORI, *Lucha contra la pornografía infantil e incriminación de actos preparatorios en el derecho penal europeo comparado*, in M. CORCOY, S. MIR PUIG (coords.), *Garantías constitucionales y derecho penal europeo (Atti del II seminario italo-spagnolo di Diritto penale)*, Barcelona, 2012, 449 ss.

[107] M. DONINI, *Modelli di illecito penale minore*, cit., 254, 260, dove afferma che rispetto a questi reati «la norma, al contempo, tutela e produce un bene giuridico».

[108] M. DONINI, *op. cit.*, 254.

[109] V. *retro*, par. 8.1.

della tutela penale[110]. Ai fini della nostra indagine è comunque opportuno richiamare i criteri in base ai quali poter stabilire la legittimità e la ragionevolezza delle fattispecie che puniscono le condotte aventi ad oggetto programmi informatici pericolosi e che sono riconducibili alla categoria dei c.d. reati di prevenzione.

### *9.1. Il rango del bene giuridico tutelato: un parametro sempre essenziale?*

L'idea che il compito principale del diritto penale sia la *tutela di beni giuridici* rappresenta ancora oggi un punto fermo della nostra penalistica, così come di quella tedesca, spagnola e latinoamericana[111]. Ne

[110] Per un quadro dei problemi dogmatici e politico-criminali che solleva l'anticipazione della tutela penale basti rinviare, per tutti, ai rilievi di G. GRASSO, *L'anticipazione della tutela penale: i reati di pericolo e di attentato*, in *Riv. it. dir. proc. pen.*, 1986, 689 ss.; M. PARODI GIUSINO, *La condotta*, cit., 687 ss., in specie 690, dove riconosce che tale materia, prestandosi per la sua complessità a valutazioni opinabili, non possa appoggiarsi su solide basi dogmatiche che abbiano la pretesa di essere vincolanti; per alcuni spunti in prospettiva comparata sui reati preparatori, v. I. SALVADORI, *I reati di possesso*, cit., 211, 234 ss., in specie 253 ss. Nella dottrina tedesca v., per tutti, G. JAKOBS, *Kriminalisierung im Vorfeld einer Rechtsgutsverletzung*, in *ZStW*, 1985, Bd. 97, H. 4, 751 ss.; W. WOHLERS, *Deliktstypen des Präventionsstrafrechts*, cit., *passim*; J. PUSCHKE, *Grund und Grenzen des Gefährdungsstrafrechts am Beispiel der Vorbereitungsdelikte*, in R. HEFENDEHL (Hrsg.), *Grenzenlose Vorverlagerung des Strafrechts?*, Berlin, 2010, 9 ss.; nonché i contributi di A. Sinn e W. Gropp, in A. SINN, W. GROPP, F. NAGY (Hrsg.), *Grenzen der Vorverlagerung in einem Tatstrafrecht. Eine rechtsvergleichende Analyse am Beispiel des deutschen und ungarischen Strafrechts*, Göttingen, 2011, 13 ss., 99 ss.; in quella di lingua inglese A.P. SIMESTER, A. VON HIRSCH, *Remote Harms and Non-constitutive Crimes*, in *Crim. Just. Ethics*, vol. 28, Issue 1, 2009, 89 ss.; ID., *Crimes, Harms, and Wrongs. On the Principles of Criminalization*, Oxford, 2011, in specie 53 ss., 70 ss.; da ultimo A. ASHWORTH, L. ZEDNER, *Prevention and Criminalization: Justifications and Limits*, in *New Crim. L. Rev.*, vol. 15, Issue 4, 2012, 542 ss.

[111] In tal senso v., per tutti, oltre al classico contributo di F. BRICOLA, voce *Teoria generale del reato*, in *Noviss. dig. it.*, XIX, Torino, 1973, 5 ss., in specie 81 ss.; G. MARINUCCI, *Fatto e scriminanti. Note dogmatiche e politico-criminali*, in *Riv. it. dir. proc. pen.*, 1983, 1190 ss., 1207 ss.; E. MUSCO, *Bene giuridico e tutela dell'onore*, Milano, 1974, 55 ss.; F. ANGIONI, *Contenuto e funzioni*, cit., 108 ss.; V. MANES, *Il principio di offensività. Canone di politica criminale, criterio ermeneutico, parametro di ragionevolezza*, Torino, 2005, *passim*; più di recente M. DONINI, *"Danno" e "offesa" nella c.d. tutela*

consegue che «il diritto penale, *se* entra in gioco, deve intervenire *nella forma* della tutela di beni»[112].

Dal riconoscimento del principio costituzionale di offensività deriva, come primo corollario, l'illegittimità di tutte quelle forme e tecniche di tutela che non puniscono una offesa (di lesione o di pericolo, non solo astratto o concreto, ma anche soltanto indiretto) di un interesse giuridico, bensì la mera violazione di norme e discipline formali, ovvero una certa tipologia d'autore (l'*hacker*, il pedofilo, il *groomer*, ecc.).

Oltre ad una selezione "in negativo" delle «forme» di tutela, il riconoscimento della centralità della protezione del bene giuridico vincola il diritto penale anche "in positivo". Esso può punire soltanto "fatti" materiali (*nullum crime sine actione*), e non le mere intenzioni o l'atteggiamento interiore (*de internis non iudicat praetor*). Ed in questo senso lo *ius puniendi* può avere ad oggetto soltanto una *condotta umana* che cagioni una *lesione* ad un interesse giuridico, o che sia comunque in grado di metterlo oggettivamente in *pericolo*.

In dottrina si è sostenuto, a ragione, che il rango del bene tutelato dovrà essere tanto più elevato quanto più il comportamento incriminato sia cronologicamente distante dalla effettiva lesione del bene[113]. Soltan-

---

*penale dei sentimenti. Note su morale e sicurezza come beni giuridici, a margine della categoria dell'"offense" di Joel Feinberg*, in A. CADOPPI (a cura di), *Laicità, valori e diritto penale. The Moral Limits of the Criminal Law. In ricordo di Joel Feinberg*, Milano, 2010, 41 ss., 49; ed in specie ID., *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in *Dir. pen. cont. - Riv. trim.*, 2014, n. 4, 4 ss., nota 1, per ampi riferimenti bibliografici anche alla dottrina straniera; D. PULITANÒ, *Offensività del reato (principio di)*, in *Enc. dir.*, Annali VIII, Milano, 2015, 665 ss. Del tutto minoritaria, nel panorama dottrinale italiano, è la tesi, che si rifà in parte a quella normativista elaborata in Germania da G. Jakobs, secondo cui il diritto penale non avrebbe ad oggetto la tutela di beni giuridici, bensì la «garanzia del mantenimento delle aspettative normative essenziali (a cementare l'identità della società) di fronte alle defraudazioni di essi, a prescindere dalle lesioni che si producono sul piano naturalistico» (in questi termini L. CORNACCHIA, *Tutela di beni giuridici* versus *tutela di norme*, in S. VINCIGUERRA, F. DASSANO (a cura di), *Scritti in memoria di Giuliano Marini*, Napoli, 2010, 217 ss., 219 ss.).

[112] M. DONINI, *"Danno" e "offesa"*, cit., 49-50; ID., *Il principio di offensività*, cit., 7. Negli stessi termini v. già G. MARINUCCI, *Fatto e scriminanti*, cit., p. 1207 ss.

[113] In tal senso v., ad es., già F. ANGIONI, *Contenuto e funzioni*, cit., 181 ss.; nella manualistica G. MARINUCCI, E. DOLCINI, *Corso*, cit., 602.

to beni di rango primario potrebbero essere tutelati in via anticipata, rispetto a condotte che rappresentano per essi solo un pericolo astratto o indiretto.

Applicando tale criterio alle norme incriminatrici esaminate in questa sede si dovrebbe concludere che molte di esse, se non tutte, debbano considerarsi costituzionalmente illegittime, dal momento che proteggono beni giuridici che non sono di rango primario. Paradigmatiche in questo senso sono le fattispecie che puniscono un ampio ventaglio di condotte (produzione, distribuzione, diffusione, cessione, detenzione, ecc.) aventi ad oggetto programmi informatici la cui funzione consiste nell'agevolare l'accesso abusivo a servizi di accesso condizionato o a pagamento (ad es. *Pay-TV*).

È innegabile che il patrimonio è un bene strumentale al pieno sviluppo della persona[114]. Ma non si può certo dire che il «nesso di strumentalità» con la personalità dell'individuo venga significativamente messo in pericolo da condotte che riducono al più le aspettative di potenziali guadagni futuri dei fornitori dei servizi criptati a pagamento. Trattandosi dunque di comportamenti che non arrecano alcuna offesa a beni patrimoniali dotati di una dimensione personalistica o comunque di pubblica utilità appare ingiustificato il ricorso allo strumento penale in una fase così arretrata[115]. Sicuramente più corretto sarebbe ricorrere, dando prevalenza alle istanze di sussidiarietà, ad altri strumenti di tutela extrapenale, ed in specie di natura civilistica o amministrativa, così come previsto, ad esempio, dal legislatore tedesco in questo ambito, se non addirittura extra-giuridiche, favorendo, ad esempio, l'adozione di TPMs.

A identiche conclusioni si deve giungere rispetto alle fattispecie previste in materia di tutela del diritto d'autore che puniscono le condotte

[114] Cfr. G. FIANDACA, *Il "bene giuridico" come problema teorico e come criterio di politica criminale*, in A. STILE (a cura di), *Bene giuridico e riforma della parte speciale*, Napoli, 1985, 3 ss., 44.

[115] Sull'opportunità di ricorrere ad altri mezzi di controllo sociale in luogo dello strumento penale per tutelare il patrimonio, in ragione del suo rango non preminente tra gli interessi meritevoli di tutela richiamati dal testo costituzionale, v., per tutti, S. MOCCIA, *Tutela penale del patrimonio e principi costituzionali*, Padova, 1988, 26 ss., 43 ss., *passim*.

aventi ad oggetto programmi informatici che permettono di aggirare o di eludere le misure tecnologiche di protezione di un'opera dell'ingegno (*software*, DVD, CD-ROM, ecc.). Tali comportamenti non cagionano un vero e proprio danno economico-patrimoniale ai titolari dei diritti di proprietà intellettuale su opere protette dal *copyright*, ma soltanto un aggiramento delle TPMs da cui può conseguire un eventuale "mancato" guadagno futuro, mediato dalla fruizione "gratuita" di tali opere.

Analoghe perplessità sorgono rispetto alle norme incriminatrici, previste ad esempio nel diritto penale tedesco (§ 263 StGB) e spagnolo (art. 264.2 CP), che puniscono la fabbricazione, la detenzione, la cessione e la diffusione di programmi informatici destinati a commettere una truffa o una frode informatica (v. *retro*, par. 6). Anche in questi casi il legislatore sarebbe ricorso illegittimamente alla sanzione criminale rispetto a comportamenti che rappresentano un mero pericolo indiretto per il bene giuridico di rango non primario del patrimonio[116].

Questa conclusione, pur muovendo da premesse astrattamente condivisibili, non tiene sufficientemente conto, però, della realtà empirica e criminologica su cui si radica la criminalità informatica ed in particolare della sua notevole *complessità tecnica*. I reati informatici commessi nel *cyberspace* (c.d. *cyber crimes* "in senso stretto") si distinguono in radice dai reati tradizionali[117].

Nella criminalità "tradizionale" nel mondo reale è/era tendenzialmente riscontrabile un rapporto di "uno a uno" (*one-to one crime*): ad una azione delittuosa (furto, omicidio, ecc.) corrisponde/va di regola una sola vittima. L'evoluzione tecnologica ha dimostrato invece come da una condotta delittuosa possano derivare molteplici offese. Basti

[116] Per una critica nei confronti di questa notevole anticipazione della tutela penale v., rispetto alla fattispecie prevista nel codice penale spagnolo, A. GALAN MUÑOZ, *El nuevo delito del artículo 248.4 CP: ¿Un adelantamiento de las barreras de protección penal del patrimonio?*, in *LL*, 2004, 1859 ss.

[117] Sulla opportuna distinzione tra reati cibernetici "in senso stretto" ed "in senso ampio" v. L. PICOTTI, *Biens juridiques protégés et techniques de formulation des infractions dans le droit pénal de l'informatique*, in *Revue Inter. Droit Pénal*, vol. 3-4, 2006, 525 ss., 529 ss. Evidenzia con acume le peculiarità della criminalità informatica rispetto a quella "tradizionale" realizzata nel mondo reale S. BRENNER, *Cybercrime Metrics: Old Wine, New Bottles?*, in *Virginia J. L. & Tech.*, vol. 9, n. 13, 2004, 1 ss.

pensare, a titolo esemplificativo, ai pericoli che derivano dall'inquinamento ambientale o ai disastri c.d. "tecnologici"[118]. Ma il mutamento di questo paradigma criminologico si coglie in modo ancora più evidente nella criminalità cibernetica (*cybercrime*).

L'incessante sviluppo delle TIC ha favorito negli ultimi anni l'"automazione" dei reati cibernetici. Essi vengono commessi mediante programmi informatici che eseguono in automatico ed in pochi secondi una molteplicità di operazioni illecite (accessi abusivi a *computer*, intercettazioni o alterazioni di dati, danneggiamento di sistemi, ecc.) senza alcuna contestuale interazione con l'uomo, se non quella meramente iniziale che si sostanzia nell'installazione ed avvio del *software*[119]. Una volta "attivati" con pochi *click* del *mouse* questi pericolosi *malware*, non solo l'intervento dell'uomo non è più necessario, ma i loro effetti dannosi o comunque pregiudizievoli sono difficilmente arrestabili, in quanto si realizzano in un brevissimo arco temporale e colpiscono in modo indiscriminato gli utenti connessi alla rete[120].

Cambia dunque completamente la prospettiva rispetto alla criminalità tradizionale. Grazie all'automazione delle TIC ad una mera azione, o meglio all'"esecuzione" di un *malware* mediante la digitazione di alcuni comandi sulla tastiera, corrispondono, di regola, molteplici reati (*one-to many crimes*)[121]. L'impiego illecito di questi *software* favorisce così la commissione di reati che assumono una dimensione c.d. di "massa" e che ledono migliaia di persone, anche fuori dai confini na-

[118] Sulle sfide che questi nuovi rischi implicano per il diritto penale si rinvia all'interessante analisi di F. CENTONZE, *La normalità dei disastri tecnologici. Il problema del congedo dal diritto penale*, Milano, 2004.

[119] In questo senso si coglie anche il limite della tradizionale concezione ontologica di azione come "movimento muscolare". Sul punto v. i condivisibili rilievi di L. PICOTTI, *Responsabilità penali in Internet*, in G. PASCUZZI (a cura di), *Diritto e informatica. L'avvocato di fronte alle tecnologie digitali*, Milano, 2002, 115 ss.; più in generale, per una critica alla concezione ontologica di azione, v. anche I. SALVADORI, *I reati di possesso*, cit., 353 ss.

[120] In tal senso parla, a ragione, di *automated crime* D.B. PARKER, *Defining Automated Crime*, in *Information System Security*, 2008, vol. 4, n. 3, 16 ss.

[121] S. BRENNER, *Cybercrime Metrics*, cit., 10.

zionali in cui opera il criminale informatico[122]. Notevoli sono, di conseguenza, le ricadute in termini di (non facile) accertamento del *locus commissi delicti* e dell'individuazione delle autorità competenti ad indagare ed accertare la commissione di tali reati cibernetici[123].

Una volta che il criminale informatico ed in specie le organizzazioni criminali che operano nel *cyberspace* hanno ottenuto la disponibilità di un sofisticato programma informatico che permette, ad esempio, di commettere una frode informatica o forme insidiose di *phishing*, potranno utilizzarlo in modo "seriale" per realizzare una moltitudine di fatti illeciti. Ma oltre a favorire la possibilità di commettere in modo "automatizzato" tali reati, questi sofisticati *software* costituiscono una seria minaccia non solo per gli interessi giuridici di un singolo individuo, ma anche per quelli di un numero potenzialmente indeterminato di persone. Un esempio concreto è utile per chiarire tale aspetto essenziale.

Si pensi, a titolo paradigmatico, ai programmi (c.d. *redirector*) che reindirizzano il traffico Internet del sistema informatico infettato verso pagine *web* apparentemente uguali a quelle che l'utente voleva consultare (*Home banking*, siti di *e-commerce*, ecc.). Quando l'utente digita i suoi dati personali (nome e cognome, *username* e *password*, numero della carta di credito, ecc.) sul sito "clonato" essi vengono automaticamente salvati sul *Server* che lo ospita e al quale accedono i criminali informatici (o c.d. *phishers*). Una volta che tali pericolosi *malware* entrano nella sfera di disponibilità di soggetti malintenzionati il rischio che vengano infettati migliaia di *computer* di ignari utenti, con conseguente sottrazione dei loro dati personali, per la commissione di future frodi è non solo assai rilevante, ma anche difficilmente evitabile.

Ma si consideri anche la pericolosità dei programmi *spyware*: una volta diffusi in rete (su pagine *web* contenenti suonerie per cellulari,

[122] Sulla categoria dei delitti c.d. massa v., nella dottrina spagnola, il classico contributo di J.A. SAINZ CANTERO, *El delito masa*, in *Anuario de Derecho Penal*, n. 24, 1971, 649 ss.

[123] In argomento v. S.W. BRENNER, *Cybercrime Jurisdiction*, in *Crime, Law and Social Change*, vol. 46, 2006, 189 ss.; J. CLOUGH, *Principles of Cybercrime*, cit., 475 ss.; da ultimo A.A. GILLESPIE, *Cybercrime. Key Issues and Debates*, Abingdon, 2016, 21 ss.

programmi gratuitamente scaricabili, giochi per *computer*, materiale pornografico, ecc.) permettono di prendere il controllo da remoto di un sistema informatico altrui e di accedere al suo contenuto o di utilizzarlo come mezzo per commettere ulteriori reati informatici (c.d. *Botnet*). Lo stesso dicasi rispetto ai *ransomware*, la cui "esecuzione" impedisce ai titolari dei sistemi "infettati" di accedere normalmente ai loro *file* e cartelle, per cui devono pagare un "riscatto" (*ransom*) per riottenerne la piena disponibilità.

È evidente dunque l'oggettiva ed elevata pericolosità di tali *software*, il cui illecito utilizzo, anche "seriale", può arrecare offesa a beni giuridici che, pur se non di rango primario (come appunto il patrimonio o la integrità di dati e di sistemi informatici "privati"), rilevano non (solo) nella dimensione individuale, bensì anche in quella collettiva. In altre parole, ad essere messo in pericolo non è soltanto l'interesse giuridico protetto del singolo individuo, ma anche quello di un numero potenzialmente indeterminato di persone, per il solo fatto che sono connesse alla rete.

Il tendenziale carattere "diffuso" dell'evento di danno o di pericolo che deriva dall'impiego di questi sofisticati *malware*, che mettono a rischio l'interesse super-individuale della sicurezza informatica[124], da cui dipende anche la salvaguardia della riservatezza informatica, nonché della integrità e disponibilità di dati e di sistemi informatici, giustifica dunque *in via eccezionale* l'intervento del diritto penale in una fase anticipata.

L'aver dimostrato come le fattispecie aventi ad oggetto pericolosi programmi informatici "a duplice uso" possano perseguire un legittimo *scopo* di tutela non basta, però, a giustificare il ricorso all'"arma" più potente di cui dispone lo Stato contro i comportamenti umani dotati di disvalore sociale. Si dovrà verificare altresì se la norma incriminatrice, così come formulata dal legislatore, sia effettivamente *adeguata* a rag-

[124] Sulla rilevanza e dimensione sociale di tale interesse v. già L. PICOTTI, *Sistematica dei reati informatici*, cit., 74 ss.; in specie ID., *Sicurezza, informatica e diritto penale*, in M. DONINI, M. PAVARINI (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, 217, 229 ss.; da ultimo I. SALVADORI, *L'accesso abusivo ad un sistema informatico*, cit., 153 ss.

giungere tale obiettivo[125]. In sostanza si tratterà di individuare, in linea con il principio di frammentarietà, quali tecniche di tutela permettano di selezionare i comportamenti che costituiscono una effettiva ed intollerabile minaccia per gli interessi giuridici meritevoli e "bisognosi" di tutela penale, distinguendosi da quelli innocui o che non raggiungono un significativo livello di pericolosità.

### *9.2. L'oggettiva connotazione offensiva del "fatto" di reato*

Nella tipizzazione normativa del "fatto" di reato devono riflettersi i connotati che caratterizzano, in termini di dannosità o di oggettiva pericolosità, la condotta o, meglio, il *Tatbestand*, quale insieme di tutti gli elementi costitutivi della fattispecie incriminatrice. Il "fatto" di reato deve dunque caratterizzarsi, sul piano oggettivo, per la sua idoneità, suscettibile di accertamento giudiziale nel caso concreto[126], a cagionare una lesione o comunque un pericolo (ancorché astratto o indiretto) per un bene giuridico[127].

---

[125] Cfr. F.C. PALAZZO, *Offensività e ragionevolezza nel controllo di costituzionalità sul contenuto delle leggi penali*, in *Riv. it. dir. proc. pen.*, 1998, 350 ss., 381 s. Sulla necessità che tra condotta incriminata e bene tutelato vi sia una *connessione funzionale* v. anche D. PULITANÒ, voce *Politica criminale*, in *Enc. dir.*, XXXIV, Milano, 1985, 73 ss., 90 s.; nella dottrina di lingua tedesca cfr. A. VON HIRSCH, W. WOHLERS, *Rechtsgutstheorie und Deliktsstruktur - zu den Kriterien fairer Zurechnung*, in R. HEFENDEHL, A. VON HIRSCH, W. WOHLERS (Hrsg.), *Die Rechtsgutstheorie. Legitimationsbasis des Strafrechts oder dogmatisches Glasperlenspiel?*, Baden-Baden, 2003, 196 ss., 197.

[126] In questi termini v. già P.J.A. FEUERBACH, *Revision der Grundsätze und Grundbegriffe des positiven peinlichen Rechts*, 2. Auf., Erfurt, 1800, rist. 1966, 12 s.; nella nostra penalistica G. MARINUCCI, *Fatto e scriminanti*, cit., 1209 ss.; da ultimo M. DONINI, *Il principio di offensività*, cit., 9 ss., 13-14; sul principio di determinatezza v., nella manualistica, G. MARINUCCI, E. DOLCINI, *Corso*, cit., 163 ss.

[127] Cfr. G. MARINUCCI, *Fatto e scriminanti*, cit., 1207 ss. Più in generale, sul significato dogmatico del concetto di "fatto tipico", v., oltre al fondamentale contributo di G. DELITALA, *Il "fatto" nella teoria generale del reato*, Milano, 1930; A. PAGLIARO, *Il fatto di reato*, Palermo, 1960; ID., *Fatto (Diritto penale)*, in *Enc. dir.*, XVI, Milano, 1967, 951 ss.; G. VASSALLI, *Il fatto negli elementi del reato*, in AA.VV., *Studi in memoria di Giacomo Delitala*, III, Milano, 1984, 1641 ss.; anche in *Riv. it. dir. proc. pen.*, 1984, 529 ss.; G. FIANDACA, *Fatto nel diritto penale*, in *Dig. disc. pen.*, V, Torino, 1991, 152 ss.

Due sono sostanzialmente le condizioni che devono verificarsi affinché si possa dire che una condotta prodromica o preparatoria determini un oggettivo e significativo aumento del rischio per il bene giuridico tutelato e non abbia alcuna giustificazione alternativa, essendo destinata alla commissione di un più grave reato (da parte del soggetto agente o di un terzo). La prima ha carattere oggettivo, mentre la seconda si connota per la sua peculiare e duplice valenza "oggettivo-soggettiva".

Da un punto di vista strettamente oggettivo, una condotta prodromica o preparatoria (*Vorfeldhandlung*) ha una valenza offensiva quando crea o aumenta il rischio di lesione per il bene giuridico tutelato (*Risikoerhöhung*)[128]. Ed essa assume una inequivocabile connotazione delittuosa (*eindeutig deliktischer Sinnbezug*) o, meglio, offensiva quando può avere soltanto il significato di semplificare o agevolare la commissione di un reato, non essendoci altra plausibile spiegazione che possa giustificarne la realizzazione[129]. Di contro, tale connotato oggettivo viene a mancare qualora il comportamento sia stato posto in essere per conseguire interessi socialmente legittimi[130].

Le esaminate norme incriminatrici che hanno ad oggetto programmi informatici utilizzabili per la commissione di un reato puniscono, come si è visto, condotte "neutre", che in sé considerate non presentano alcun disvalore sociale. Il loro carattere di pericolosità andrà dunque individuato sulla base della relazione che viene ad instaurarsi rispetto ad altri *elementi costitutivi* del "fatto" di reato. Ed in questo senso le condotte prodromiche o preparatorie tipizzate si "colorano" in termini di intrinseca pericolosità per un bene giuridico quando hanno ad oggetto un programma informatico che può essere effettivamente impiegato per commettere un fatto costitutivo di reato[131].

---

[128] W. FRISCH, *Tatbestandsmäßiges Verhalten und Zurechnung des Erfolgs*, Heidelberg, 1988, 293.

[129] W. FRISCH, *op. cit.*, 281, in specie 289; in senso conf. W. WOHLERS, *Deliktstypen des Präventionsstrafrechts*, cit., 335; G. DUGGTE, *Vorbereitung eines Computerbetruges*, cit., 301.

[130] W. FRISCH, *op. cit.*, 307.

[131] Cfr. A. ALBRECHT, *op. cit.*, 277 s., che parla anche di idoneità alla commissione di un delitto (*Eignung zur Deliktsbegehung*).

Come si è avuto modo di evidenziare, nessuna delle tecniche di formulazione normativa impiegate a livello sovranazionale riesce a determinare con sufficiente precisione quali siano i programmi informatici che rappresentano di per sé un pericolo per un determinato bene[132]. Eccessivamente restrittiva, oltre che in contrasto con le caratteristiche tecniche dei nuovi dispositivi, sarebbe la scelta di limitare la sanzione criminale ai programmi che siano *esclusivamente* destinati alla commissione di un reato[133]. Non solo non è facile determinare in sede processuale se un *software* possa essere utilizzato soltanto per scopi criminosi: limitando l'oggetto materiale ai programmi unicamente destinati a commettere un reato, si finirebbe con l'escludere automaticamente la rilevanza penale delle condotte che riguardano i ben più numerosi programmi multifunzione, e di cui una consista appunto nel permettere di realizzare un fatto illecito. L'impiego di questa tecnica di formulazione destinerebbe dunque la previsione legale ad un mero ruolo simbolico.

Sicuramente più corretta è la scelta di selezionare quei programmi informatici che si caratterizzano, su un piano oggettivo, per la loro *idoneità* a commettere determinati reati (intercettazioni di dati, accesso abusivo ad un sistema informatico protetto, falsificazione di mezzi di pagamento, violazioni del *copyright*, ecc.). La disponibilità di tali *software*, siano essi multifunzione o multiscopo, agevolerebbe o faciliterebbe all'agente o ad un terzo la commissione di un determinato reato.

Il ricorso a questa tecnica di tipizzazione normativa, suscettibile di per sé di rispettare i fondamentali principi di determinatezza-tassatività e di precisione, avrebbe l'indubbio vantaggio di assicurare l'effettività della norma incriminatrice, garantendone la possibilità di applicazione in sede processuale[134].

Non tutte le condotte che hanno ad oggetto un programma informatico di per sé *idoneo* a commettere un reato hanno del resto un identico grado di disvalore sociale. Quelle che si sostanziano in una abusiva

---

[132] V. *retro*, par. 5.3.

[133] Cfr., rispetto a talune fattispecie previste nel codice penale spagnolo, *retro*, par. 6.

[134] Sul principio politico-criminale di effettività v., per tutti, gli acuti rilievi di C.E. PALIERO, *Il principio di effettività nel diritto penale*, in *Riv. it. dir. proc. pen.*, 1990, 430 ss.; ID., *Il principio di effettività nel diritto penale*, Napoli, 2011.

"messa a disposizione" ad un numero indeterminato di persone di un pericoloso *software* determinano un maggiore aumento del rischio per i beni giuridici tutelati[135]. A seguito della distribuzione mediante un programma *P2P* o della diffusione di un *malware* in rete chiunque potrebbe impossessarsene ed utilizzarlo per fini illeciti. Difficile risulterebbe inoltre la sua soppressione, data la facilità con la quale potrebbe essere duplicato.

Minore sarà, di contro, il grado di pericolosità insito nelle condotte che consistono nell'esercizio di una signoria su tali *software*[136]. In questo caso vi sarebbe soltanto la possibilità di impiegare il programma informatico per scopi illeciti o di permettere a terzi di servirsi o "agganciarsi" a tale condotta per raggiungere propositi criminosi[137]. Di conseguenza, sarà opportuno che la cornice edittale prevista per i menzionati reati non sia contenuta entro margini troppo ristretti. Soltanto in questo modo sarà garantita la possibilità al giudice di dosare la pena in proporzione al diverso grado di pericolo insito in ciascun "fatto" di reato.

La mera connotazione in termini di oggettiva *idoneità* dell'oggetto materiale della condotta tipica (di produzione, di procacciamento, di cessione, ecc.) non basta, però, a selezionare gli atti prodromici o preparatori *tipicamente* e *generalmente* connotati da un inequivocabile significato offensivo. Un *system administrator* potrebbe avere la disponibilità di un pericoloso *malware* non per finalità illecite, ma per studiarne la struttura e sviluppare un "antidoto" (ad es. un anti-virus o un *firewall*), che riesca a neutralizzarne gli effetti dannosi, così da garantire la sicurezza di una rete aziendale. Se si punisse il mero fatto di disporre di un programma informatico idoneo a commettere un reato o di metterlo a disposizione a soggetti determinati (ad es. ad una *Software House*) si finirebbe per proibire gran parte delle attività poste in essere dagli esperti del settore IT per migliorare il livello della sicurezza informatica, che di per sé non hanno alcun disvalore sociale e non aumentano in modo significativo il rischio di lesione di un bene giuridico.

[135] Su tali condotte v. *retro*, par. 8.2.

[136] V. *retro*, par. 8.1.

[137] Cfr. W. FRISCH, *Tatbestandsmäßiges Verhalten*, cit., 265.

Per evitare una eccessiva criminalizzazione, si dovranno *selezionare* con maggior precisione quei "fatti" aventi carattere preparatorio o agevolatore che mettono oggettivamente in pericolo (ancorché in modo indiretto) i beni giuridici tutelati. A tal fine si dovrà richiedere, da un punto di vista "soggettivo", che il fatto venga posto in essere con l'intenzione, meglio con il "fine" di commettere un fatto illecito ovvero di cagionare un evento/risultato lesivo[138].

Secondo autorevole dottrina, soltanto mediante la previsione espressa dell'intenzione del soggetto di utilizzare quel determinato "oggetto" per una finalità illecita il fatto tipizzato acquisterebbe un inequivocabile significato delittuoso[139]. Il fine criminoso che sorregge la condotta dell'agente verrebbe a palesare la sua intenzione di commettere con quell'oggetto illecito (armi, esplosivi, *malware*, ecc.) un dato comportamento costitutivo di reato, arricchendo, sul piano (esclusivamente) "soggettivo", la descrizione del fatto-base di reato. La conclusione sistematica cui giunge questo orientamento, pur muovendo da condivisibili premesse, non può però essere accolta.

La previsione del fine illecito che deve sorreggere il fatto-base, prima ancora di incidere sull'elemento "soggettivo" di fattispecie, svolge una fondamentale funzione «tipizzante»[140]. Mediante la tipizzazione normativa di uno specifico "fine" di commettere un reato ovvero di cagionare un evento/risultato lesivo si selezionano, già sul piano «oggettivo», le condotte che sono effettivamente *strumentali* alla realizzazione del risultato (illecito) che persegue il soggetto agente.

Evidente è infatti il rilievo che assume il "nesso teleologico" che deve legare la condotta o il fatto-base (di produzione, procacciamento, detenzione, diffusione, ecc.) avente ad oggetto un pericoloso *software* con lo scopo illecito preso di mira. Il "fine" specifico di commettere

---

[138] Cfr. A. ALBRECHT, *op. cit.*, 278, che parla al riguardo di *Verwendungsabsicht*, pur connotandolo in termini soltanto "soggettivi" e non, come da noi proposto, in termini di "tipizzazione" del fatto-base oggettivo.

[139] W. FRISCH, *Tatbestandsmäßiges Verhalten*, cit., 319; in senso conf. U. SIEBER, *Legitimation und Grenzen von Gefährdungsdelikten*, cit., 361.

[140] È questa la condivisibile conclusione alla quale giunge, sulla base di una articolata e rigorosa argomentazione dogmatica e politico-criminale, L. PICOTTI, *Il dolo specifico*, cit., 501 ss.

quel determinato reato (o risultato/evento lesivo) che deve sorreggere la condotta oggettivamente descritta non solo ne implica la previa rappresentazione da parte dell'agente, ma anche che questa abbia una efficacia «causale» sul suo agire esterno[141]. In altre parole, il comportamento strumentale da lui posto in essere costituisce già la parziale «realizzazione» di quello scopo illecito, in quanto è il «mezzo» necessario per il verificarsi del "risultato" da lui perseguito[142]. Il fine specifico di commettere un fatto costitutivo di reato ovvero lesivo concorre in definitiva a puntualizzare l'oggettivo significato *preparatorio* che assume la condotta-base in quanto *strumentale* al raggiungimento di quel risultato. Soltanto qualora sussista questa connessione teleologica con il fine tipizzato si potrà dire che la condotta-base è tipica e quindi penalmente rilevante.

Mediante il ricorso a questa peculiare tecnica di formulazione normativa diventa possibile assicurare al settore IT di continuare a sviluppare e testare in modo legittimo i *software* necessari per verificare la vulnerabilità dei sistemi informatici e di studiare le minacce rappresentate dai *malware*. Il tecnico informatico che produce un programma per "crackare" le *password* non sarebbe dunque punito, qualora con la sua condotta perseguisse il legittimo fine di simulare un attacco ad un *computer* per studiarne la resistenza alle minacce che provengono dalla rete. Rispetto a tali comportamenti mancherebbe invero quel rapporto di mezzo a fine tra la disponibilità di un programma informatico "a duplice uso" ed il fine di commettere un determinato reato ovvero di cagionare un risultato/evento *contra ius*.

In alcuni casi, però, la previsione, nella descrizione normativa del fatto tipico, del fine specifico di commettere un reato (di accesso abusivo ad un sistema informatico protetto da misure di sicurezza, di danneggiamento di dati o di sistemi informatici, ecc.) o di cagionare un risultato/evento lesivo (ad es. arrecare ad altri un danno) potrebbe restringere eccessivamente l'area del penalmente rilevante. Si pensi, a titolo esemplificativo, allo sviluppatore informatico che, dopo aver creato un sofisticato *malware* che permette di vulnerare i sistemi di sicurez-

[141] L. PICOTTI, *op. cit.*, 501.
[142] L. PICOTTI, *op. cit.*, 502.

za di un sistema operativo, decida di cederlo o venderlo abusivamente ad un terzo o comunque di metterlo a disposizione di altri in rete[143].

In questo caso la sua condotta non sarebbe sussumibile nell'alveo della fattispecie a dolo specifico, dal momento che non persegue il fine di commettere o di far commettere un reato ovvero di arrecare ad altri un danno. Anche qualora accettasse il rischio che il soggetto al quale cede il programma possa utilizzarlo per scopi illeciti non sarebbe integrato il fine specifico. La «causa» del suo agire non sarebbe, infatti, la realizzazione del "fine" espressamente tipizzato dalla previsione legale, ma il perseguimento di un diverso interesse "di parte" (ad es. di profitto) il cui conseguimento non dipende dal realizzarsi di quel fine specifico[144]. La condotta, pur creando sicuramente un pericolo per i beni giuridici tutelati, rimarrebbe impunita.

Per evitare che si crei una lacuna normativa, si dovrebbero incriminare in modo autonomo le condotte che consistono nel mettere *abusivamente* a disposizione di terzi un *software* oggettivamente *idoneo* a commettere un reato[145]. Rispetto a tali comportamenti basterebbe dunque richiedere che il fatto sia sorretto dalla "volontà consapevole" di diffondere *senza autorizzazione* a soggetti indeterminati un programma informatico che è idoneo a commettere un reato (di accesso abusivo ad un sistema informatico, di intercettazione di dati informatici, ecc.). Soltanto in questo modo sarebbe possibile punire anche quelle condotte che, pur non essendo in sé strumentali alla realizzazione di un reato da parte dello stesso soggetto agente o di un terzo, determinano comunque un illegittimo e significativo aumento del rischio per i beni giuridici tutelati e non rientrano nel normale svolgimento delle attività legittime

[143] Ipotesi questa tutt'altro che di scuola e che è stata opportunamente riconosciuta dal nostro legislatore all'art. 615-*quater* c.p., nella parte in cui punisce condotte concernenti codici e programmi idonei ad accedere abusivamente ad un sistema informatico protetto da misure di sicurezza «al fine di procurare a sé o ad altri un profitto».

[144] Questo non significa che il dolo eventuale sia incompatibile con le fattispecie a dolo specifico, qualora abbia ad oggetto elementi della fattispecie incriminatrice diversi da quelli finalistici "specifici". Si pensi, a titolo paradigmatico, all'"altruità" della cosa nel delitto di furto. In argomento v. già M. GALLO, voce *Dolo (dir. pen.)*, in *Enc. dir.*, XIII, Milano, 1964, 750 ss., 794; ed in specie L. PICOTTI, *Il dolo specifico*, cit., 595 ss., 598 ss., 610.

[145] Cfr. A. ALBRECHT, *op. cit.*, 270, 278.

e socialmente adeguate dei soggetti che operano quotidianamente nel settore IT per migliorare il livello della sicurezza informatica.

### *9.3. La necessità e la proporzionalità della sanzione penale*

Da ultimo, si dovrà verificare, in una logica di *extrema ratio*, la effettiva necessità o "bisogno" di ricorrere allo strumento penale per punire, nell'ambito esaminato, meri atti prodromici o preparatori alla commissione di più gravi reati[146]. Ed in tal senso occorrerà stabilire, nel rispetto del fondamentale principio di sussidiarietà, se non sia possibile prevenire i rischi che derivano dalle condotte aventi ad oggetto un *software* idoneo a commettere un reato, ricorrendo a strumenti e misure di controllo che comprimano in misura minore gli spazi di libertà del singolo (ad es. sanzioni civili o amministrative, misure di sicurezza, dispositivi tecnologici di protezione, ecc.).

Il ricorso allo strumento penale in questo ambito appare, però, inevitabile, se si tiene conto della oggettiva pericolosità dei programmi *malware* e del rischio che una loro diffusione possa favorire una criminalità di massa[147]. Troppo elevati sono i rischi che possono derivare alle infrastrutture critiche (traffico aereo, ferroviario, ospedali, centrali elettriche e nucleari, ecc.), il cui regolare funzionamento dipende dalla integrità e disponibilità di dati e di sistemi informatici, dalla distribuzione e circolazione indiscriminata di queste insidiose "armi cibernetiche", ma anche ai beni giuridici di un numero potenzialmente indeterminato di persone per il mero fatto che sono connesse ad Internet.

Nella determinazione del trattamento sanzionatorio dei menzionati fatti di reato si dovrà comunque tener conto dell'esiguo significato lesivo che essi assumono rispetto alla effettiva offesa (in termini di lesione ovvero di diretta messa in pericolo in grado più prossimo) del bene tutelato dalla norma incriminatrice e che deriva dalla realizzazione del risultato cui tendono (danneggiamento di dati o sistemi informatici, in-

[146] Sulla meritevolezza ed il bisogno di pena quali fattori di «legittimazione ultima del tipo astratto di reato» (e pertanto della natura *penale* del divieto) e la «sostanza» di cui il reato si nutre v. gli autorevoli rilievi di M. ROMANO, *«Meritevolezza di pena», «bisogno di pena» e teoria del reato*, in *Riv. it. dir. proc. pen.*, 1992, 39 ss., 50.

[147] Cfr. *retro*, par. 9.1.

tercettazioni di dati, falsificazione di monete o sistemi di pagamento, frodi, ecc.)[148].

Sembra dunque in contrasto con il principio di proporzionalità il trattamento sanzionatorio (reclusione da 1 a 5 anni e multa) previsto dal nostro legislatore per le condotte aventi ad oggetto programmi informatici destinati esclusivamente alla falsificazione di monete (art. 461 c.p.). Tale fatto, che costituisce un atto prodromico del più grave reato di alterazione di monete (art. 454 c.p.), viene punito con la stessa pena stabilita per quest'ultimo. Si tratta dunque di una irragionevole sperequazione sanzionatoria. La pena prevista per un reato che sanziona in via autonoma gli atti prodromici di un più serio reato (ad es. artt. 435, 455, 462 c.p.) deve essere necessariamente inferiore rispetto a quella prevista per quest'ultimo e, comunque, proporzionata a quella inflitta per il tentativo del reato a cui tende[149].

Una violazione del principio di proporzione sussiste anche tra le fattispecie, sopra analizzate, previste in materia di tutela del diritto d'autore. Con lo stesso trattamento sanzionatorio (reclusione da 6 mesi a 3 anni e multa) previsto, ad esempio, per il più grave reato di furto, vengono puniti, in base ai menzionati artt. 171-*ter*, co, 1, lett. f-*bis*), e 171-*ter*, co. 1, lett. f), l. dir. aut., meri atti prodromici o preparatori rispetto alla futura commissione di reati di abusiva duplicazione o riproduzione di un'opera dell'ingegno, ecc., che incidono sulle TPMs e che offendono soltanto in via *mediata* gli interessi patrimoniali dei titolari delle

[148] Proprio per questo motivo risulta eccessivamente sproporzionato il trattamento sanzionatorio previsto dal codice penale spagnolo per le condotte aventi ad oggetto programmi informatici destinati alla commissione di un reato di cui ai citati artt. 270.3 CP sp. (ora art. 270.6 CP sp., dopo la novella del 2015), 248.2, let. b), e 400 CP sp. Cfr. i rilievi critici di M. CORCOY BIDASOLO, *Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos*, in *Eguzkilore. Cuaderno del Instituto Vasco de Criminología*, 2007, n. 21, 7 ss., 16; F.J. ÁLVAREZ GARCÍA, *Estafa (I)*, in ID. (dir.), *Derecho penal español*, *Parte especial (II)*, Valencia, 2011, 354.

[149] In questo senso v. anche il par. II.5 della risoluzione sull'espansione delle forme di preparazione e di partecipazione al reato, adottata dall'Associazione Internazionale di Diritto Penale (AIDP) al XVIII congresso internazionale di diritto penale, tenutosi a Istanbul dal 20 al 27 settembre 2009. Il testo originale della risoluzione è consultabile al sito *http://www.aidpitalia.org*.

opere tutelate dal diritto d'autore. Meglio dunque avrebbe fatto il nostro legislatore a ricorrere allo strumento penale per punire esclusivamente le condotte concernenti *software* destinati ad agevolare o facilitare l'aggiramento delle misure di protezione poste a tutela delle opere di ingegno commesse su scala commerciale (*on a commercial scale*), così come previsto dall'art. 10 della Convenzione *Cybercrime*.

L'eccessiva ed irragionevole anticipazione della tutela penale nell'ambito della normativa sul *copyright* emerge ancora di più se si tiene conto che il legislatore, in modo criticabile, ha assicurato alla componente economico-patrimoniale dei diritti di proprietà intellettuale una protezione molto più energica, rispetto a quella di beni di rango superiore. Si pensi, ad esempio, alle aggressioni contro gli interessi fondamentali dell'integrità fisica o della vita, rispetto ai quali non vengono puniti meri atti preparatori alla loro offesa (come il procurarsi, l'acquistare o il detenere veleno o un arma "al fine di" uccidere una persona)[150].

Si tratta dunque di scelte punitive che contrastano con il "divieto di eccesso" (*Übermaßverbot*), dal momento che non vi è un equilibrio tra il sacrificio della libertà personale e dei diritti fondamentali del destinatario della sanzione penale e lo scopo di tutela che viene perseguito.

Rispetto alle menzionate fattispecie criminose, la cui pena risulta sproporzionata sia per la esigua gravità dell'offesa che per il basso rango del bene giuridico tutelato, sarà sicuramente più corretto il ricorso, in forza del fondamentale principio di sussidiarietà, a strumenti di tutela di natura civilistica ovvero a sanzioni pecuniarie o amministrative. Ed è questa la condivisibile scelta adottata, ad esempio, dal legislatore tedesco, che ha ritenuto di punire con una sanzione amministrativa le condotte aventi ad oggetti programmi informatici destinati a violare misure di protezione di opere protette dal *copyright*, trattandosi di comporta-

[150] Nel tutelare in via anticipata i menzionati beni giuridici il legislatore tende a ricorrere alla tecnica di incriminazione dei "reati di ostacolo". Questi ultimi si contraddistinguono dai reati preparatori in senso stretto, dal momento che non richiedono, sul piano "soggettivo", che il soggetto agente si prefigga la commissione di un futuro reato ovvero intenda perseguire uno scopo illecito. Sul punto v. I. SALVADORI, *I reati di possesso*, cit., 260 s.

menti che arrecano una offesa non grave ad un bene giuridico di rango non elevato[151].

## *10. Considerazioni finali e proposte* de lege ferenda

Volendo tirare le somme dalle considerazioni sin qui svolte ci pare di poter affermare che per una corretta incriminazione delle condotte che hanno ad oggetto *dual-use software* e, più in generale, prodotti a "doppio uso" (grimaldelli, armi, sostanze batteriologiche, "informazioni", ecc.), si debbano rispettare sostanzialmente tre requisiti.

In primo luogo il legislatore dovrebbe descrivere in termini pregnanti l'oggetto materiale del reato. Questo non significa che si debbano punire soltanto i programmi informatici che sono *specificamente* o *esclusivamente* destinati a commettere un reato[152]. Mediante il ricorso a questa discutibile tecnica di tipizzazione legislativa, si finirebbe per restringere eccessivamente l'ambito della tutela penale, relegando le menzionate norme incriminatrici ad un ruolo simbolico. Non è un caso del resto che l'applicazione giurisprudenziale di queste fattispecie, pur a distanza di molti anni dalla loro entrata in vigore, sia ancora molto scarsa o praticamente nulla.

Sicuramente più corretta appare la scelta di punire le condotte che hanno ad oggetto programmi informatici che per la loro intrinseca natura siano oggettivamente *idonei* a commettere un reato. Ed in questo senso condivisibile è la tecnica di formulazione normativa impiegata dal nostro legislatore all'art. 615-*quater* c.p., laddove ha punito i "dispositivi" che sono *idonei* a commettere un accesso abusivo ad un sistema informatico protetto da misure di sicurezza. Lo stesso dicasi per la scelta del legislatore tedesco, di incriminare le condotte aventi ad oggetto i *software* che per loro natura sono *idonei* a commettere («die ihrer Art nach zur Begehung […] geeignet sind») una falsificazione di monete o valori bollati (§ 149, Abs. 1, Nr. 1 StGB).

---

[151] §§ 95a, Abs. 3, 111a Abs. 1, b), UrhG.

[152] È questa, ad es., la tecnica di formulazione normativa impiegata dal nostro legislatore all'art. 461, co. 1, c.p.

Ai fini di una corretta delimitazione dell'area del penalmente rilevante non è, però, sufficiente richiedere che l'oggetto materiale del reato venga connotato, dal punto di vista oggettivo, in termini di *idoneità* a commettere un reato. In questo modo si finirebbero per colpire indiscriminatamente tutte le condotte (di produzione, detenzione, cessione, distribuzione, ecc.) che hanno ad oggetto un *software* che può essere utilizzato per fini illeciti[153].

Anche gli esperti informatici e coloro che lavorano nel settore IT acquistano, sviluppano, utilizzano o cedono programmi informatici idonei a commettere un reato per realizzare controlli di sicurezza (*Security Testing*), per scopi dimostrativi o per finalità di studio e creazione di programmi in grado di contrastare le nuove minacce che provengono dal *web*. Anch'essi, al pari dei criminali informatici, possono dunque produrre, procurarsi, acquistare o impiegare tali *software* per porre in essere "attacchi" a sistemi informatici (accessi abusivi ad un *computer*, intercettazioni di comunicazioni tra sistemi telematici, danneggiamenti di dati o di sistemi informatici, violazioni delle TPMs, ecc.).

Affinché le condotte aventi ad oggetto un programma informatico *idoneo* a commettere, anche in modo seriale, un reato assumano un oggettivo connotato offensivo e contribuiscano ad aumentare in modo significativo il pericolo per i beni giuridici tutelati, si dovrà richiedere, sul piano "soggettivo", che il fatto venga posto in essere *al fine di* utilizzare quel determinato oggetto pericoloso per la commissione di un fatto costitutivo di reato o per cagionare un evento/risultato lesivo.

Contrariamente a quanto viene ancora oggi sostenuto nella nostra prevalente dottrina, la previsione di un fine specifico che sorregga il fatto-base, prima ancora di qualificare l'elemento soggettivo e la colpevolezza, permette di *selezionare* i fatti che risultano oggettivamente *strumentali* al perseguimento del fine illecito, che costituisce la "causa", *rectius* "interesse" causale che realmente determina il soggetto ad agire. Mediante il ricorso a questa peculiare tecnica normativa si tipizza la *proiezione conflittuale* della condotta dell'agente nei confronti del contrapposto interesse facente capo al soggetto passivo anche se di per

[153] Sul significato dei c.d. *dual-use software*, assunto in questa sede, v. *retro*, par. 3.

sé indeterminato[154]. Ponendo in essere quella determinata condotta per commettere fatti costitutivi di reato (o risultati lesivi) che costituiscono l'oggetto del fine espressamente richiamato dalla previsione legale, il soggetto agente mette già in "pericolo" il contrapposto interesse, appartenente ad un individuo o ad un gruppo indeterminato di persone.

La previsione del "fine" di commettere un reato o di cagionare un risultato lesivo, che deve essere legato alla condotta-base avente ad oggetto un *software* idoneo a perpetrare (anche in modo seriale) un reato, potrebbe avere però l'effetto di restringere eccessivamente l'area del penalmente rilevante. Le condotte che consistono nella "messa a disposizione" di un programma informatico pericoloso a soggetti indeterminati, non sorrette dal fine di commettere un reato, non sarebbero invero punibili, pur potendo costituire una seria minaccia per i beni giuridici tutelati. Sarebbe dunque opportuno punire in modo autonomo i comportamenti sorretti dalla mera "volontà consapevole" (dolo generico) di mettere a disposizione di un numero indeterminato di persone un programma informatico oggettivamente idoneo a commettere un reato.

In terzo ed ultimo luogo si dovrebbe richiedere, sul piano della descrizione del *Tatbestand*, che i "fatti" di reato aventi ad oggetto un *software* "a duplice uso" vengano posti in essere *in mancanza di autorizzazione* o *abusivamente*[155]. Mediante questa opportuna clausola di antigiuridicità speciale si assicurerebbe ai tecnici che lavorano in ambito IT di operare in modo lecito e di perseguire i loro legittimi scopi di elevare lo standard di sicurezza informatica, nell'interesse anche della collettività e della società, sempre più dipendente dal corretto e sicuro funzionamento dei sistemi informatici e telematici, ormai interconnessi alla rete *Internet*.

---

[154] Sottolinea come alla base di ogni fattispecie incriminatrice debba esserci un rapporto conflittuale di interessi F.C. PALAZZO, *I confini della tutela penale: selezione dei beni e criteri di criminalizzazione*, in *Riv. it. dir. proc. pen.*, 1992, 453 ss., 463; nonché L. PICOTTI, *Il dolo specifico*, cit., 547 ss.; più di recente ID., *La nozione di «criminalità informatica»*, cit., 838 ss.

[155] È interessante segnalare in tal senso come il legislatore francese abbia opportunamente punito soltanto le condotte concernenti dati o programmi informatici destinati a commettere un reato contro la riservatezza informatica, la disponibilità ovvero l'integrità di dati o di sistemi informatici, poste in essere «sans motif légitime, notamment de recherche ou de sécurité informatique» (art. 323-3-1 CP).

# GLI AUTORI

*Roberto Wenin*
Responsabile scientifico del progetto di ricerca «Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali», Assegnista di ricerca in Diritto Penale e Dottore di ricerca in Studi Giuridici Comparati ed Europei, Università degli Studi di Trento, Avvocato

*Gabriele Fornasari*
Professore di Diritto Penale, Università degli Studi di Trento

*Giuseppe Nesi*
Preside della Facoltà di Giurisprudenza e Professore di Diritto Internazionale, Università degli Studi di Trento

*Antonio Cavaliere*
Professore di Diritto Penale, Università degli Studi di Napoli Federico II

*Roberto Bartoli*
Professore di Diritto Penale, Università degli Studi di Firenze, Avvocato

*Ilaria Marchi*
Dottore di ricerca in Studi Giuridici Comparati ed Europei, Università degli Studi di Trento, Avvocato

*Beniamino Migliucci*
Presidente dell'Unione delle Camere Penali Italiane, Avvocato

*Guido Salvini*
GIP presso il Tribunale di Milano

*Mariateresa Fiocca*
Professoressa di Economia, Scuola Nazionale dell'Amministrazione – SNA, Presidenza del Consiglio

*Gabriella Di Paolo*
Professoressa di Diritto Processuale Penale, Università degli Studi di Trento

*John A.E. Vervaele*
Professore di Diritto Penale dell'Economia e Diritto Penale Europeo, Università di Utrecht, Professore di Diritto Penale Europeo, College of Europe, Presidente dell'Association Internationale de Droit Pénal

*Marcello Daniele*
Professore di Diritto Processuale Penale Comparato, Università degli Studi di Padova

*Federica Iovene*
Dottore di ricerca in Studi Giuridici Comparati ed Europei, Università degli Studi di Trento, Magistrato Ordinario in Tirocinio

*Lorenzo Picotti*
Professore di Diritto Penale, Università degli Studi di Verona, Avvocato

*Roberto Flor*
Ricercatore in Diritto Penale e Professore aggregato di Diritto Penale dell'Informatica e Dritto Penale Internazionale, Università degli Studi di Verona, Coordinatore scientifico dell'Observatory on Cybercrime – Dipartimento di Scienze Giuridiche dell'Università degli Studi di Verona

*Ivan Salvadori*
Assegnista di ricerca in Diritto Penale e Professore a contratto di Diritto penale, Università degli Studi di Verona, Professore a contratto di Diritto Penale dell'Informatica, Universidad Oberta de Catalunya

**COLLANA**
**'QUADERNI DELLA FACOLTÀ DI GIURISPRUDENZA'**

**UNIVERSITÀ DEGLI STUDI DI TRENTO**

1. *L'applicazione delle regole di concorrenza in Italia e nell'Unione europea. Atti del IV Convegno Antitrust tenutosi presso la Facoltà di Giurisprudenza dell'Università di Trento* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2014)

2. *Dallo status di cittadino ai diritti di cittadinanza* - (a cura di) FULVIO CORTESE, GIANNI SANTUCCI, ANNA SIMONATI (2014)

3. *Il riconoscimento dei diritti storici negli ordinamenti costituzionali* - (a cura di) MATTEO COSULICH, GIANCARLO ROLLA (2014)

4. *Il diritto del lavoro tra decentramento e ricentralizzazione. Il modello trentino nello spazio giuridico europeo* - (a cura di) ALBERTO MATTEI (2014)

5. *European Criminal Justice in the Post-Lisbon Area of Freedom, Security and Justice* - JOHN A.E. VERVAELE, with a prologue by Gabriele Fornasari and Daria Sartori (Eds.) (2014)

6. *I beni comuni digitali. Valorizzazione delle informazioni pubbliche in Trentino* - (a cura di) ANDREA PRADI, ANDREA ROSSATO (2014)

7. *Diplomatici in azione. Aspetti giuridici e politici della prassi diplomatica nel mondo contemporaneo* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2015)

8. *Il coordinamento dei meccanismi di stabilità finanziaria nelle Regioni a Statuto speciale* - (a cura di) ROBERTO TONIATTI, FLAVIO GUELLA (2014)

9. *Reti di libertà. Wireless Community Networks: un'analisi interdisciplinare* - (a cura di) ROBERTO CASO, FEDERICA GIOVANELLA (2015)

10. *Studies on Argumentation and Legal Philosophy. Further Steps Towards a Pluralistic Approach* - (Ed. by) MAURIZIO MANZIN, FEDERICO PUPPO, SERENA TOMASI (2015)

11. *L'eccezione nel diritto. Atti della giornata di studio (Trento, 31 ottobre 2013)* - (a cura di) SERGIO BONINI, LUCIA BUSATTA, ILARIA MARCHI (2015)

12. José Luis Guzmán D'Albora, *Elementi di filosofia giuridico-penale* - (a cura di) GABRIELE FORNASARI, ALESSANDRA MACILLO (2015)

13. *Verso nuovi rimedi amministrativi? Modelli giustiziali a confronto* - (a cura di) GIANDOMENICO FALCON, BARBARA MARCHETTI (2015)

14. *Convergences and Divergences between the Italian and the Brazilian Legal Systems* - (Ed. by) GIUSEPPE BELLANTUONO, FEDERICO PUPPO (2015)

15. *La persecuzione dei crimini internazionali. Una riflessione sui diversi meccanismi di risposta. Atti del XLII Seminario internazionale di studi italo-tedeschi, Merano 14-15 novembre 2014 - Die Verfolgung der internationalen Verbrechen. Eine Überlegung zu den verschiedenen Reaktionsmechanismen. Akten des XLII. Internationalen Seminars deutsch-italienischer Studien, Meran 14.-15. November 2014* - (a cura di / herausgegeben von) ROBERTO WENIN, GABRIELE FORNASARI, EMANUELA FRONZA (2015)

16. *Luigi Ferrari Bravo. Il diritto internazionale come professione* - (a cura di) GIUSEPPE NESI, PIETRO GARGIULO (2015)

17. *Pensare il diritto pubblico. Liber Amicorum per Giandomenico Falcon* - (a cura di) MAURIZIO MALO, BARBARA MARCHETTI, DARIA DE PRETIS (2015)

18. *L'applicazione delle regole di concorrenza in Italia e nell'Unione europea. Atti del V Convegno biennale Antitrust. Trento, 16-18 aprile 2015* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2015)

19. *From Contract to Registration. An Overview of the Transfer of Immoveable Property in Europe* - (ed. by) ANDREA PRADI (2015)

20. *Diplomatici in azione. Aspetti giuridici e politici della prassi diplomatica nel mondo contemporaneo. Volume II* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2016)

21. *Democrazie e religioni: libertà religiosa, diversità e convivenza nell'Europa del XXI secolo. Atti del convegno nazionale Adec Trento, 22 e 23 ottobre 2015* - (a cura di) ERMINIA CAMASSA (2016)

22. *Modelli di disciplina dell'accoglienza nell'"emergenza immigrazione". La situazione dei richiedenti asilo dal diritto internazionale a quello regionale* - (a cura di) JENS WOELK, FLAVIO GUELLA, GRACY PELACANI (2016)

23. *Prendersi cura dei beni comuni per uscire dalla crisi. Nuove risorse e nuovi modelli di amministrazione* - (a cura di) MARCO BOMBARDELLI (2016)

24. *Il declino della distinzione tra diritto pubblico e diritto privato. Atti del IV Congresso nazionale SIRD. Trento, 24-26 settembre 2015* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE GRAZIADEI (2016)

25. Fiat Intabulatio. *Studi in materia di diritto tavolare con una raccolta di normativa* - (a cura di) ANDREA NICOLUSSI, GIANNI SANTUCCI (2016)

26. *Le definizioni nel diritto. Atti delle giornate di studio, 30-31 ottobre 2015* - (a cura di) FULVIO CORTESE, MARTA TOMASI (2016)

27. *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali. Atti del convegno. Trento, 2 e 3 ottobre 2015* - (a cura di) ROBERTO WENIN, GABRIELE FORNASARI (2017)