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.

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.