Università degli Studi di Ferrara

DOTTORATO DI RICERCA IN

Diritto dell'Unione europea ed Ordinamenti nazionali

CICLO XXXV

COORDINATORE: Prof. De Cristofaro Giovanni

Il delicato rapporto fra diritto penale e nuove tecnologie nel contrasto al cyberterrorismo.
Il quadro normativo nazionale ed eurounitario.

Settore Scientifico Disciplinare IUS/17

Dottorando
Dott. Benato Edoardo

Tutore
Prof.ssa Bernasconi Costanza

Anni 2019/2022

SOMMARIO

PREMESSA

L'oggetto di indagine del presente lavoro è duplice: l'inquadramento giuridico del *cyberterrorismo*, al fine di fornirne una definizione penalmente rilevante; la ricerca degli strumenti per la sua *prevenzione*.

La rivoluzione digitale, iniziata sul finire degli anni '50 del XX secolo, superata la fase dell'*informatica*, è ormai inesorabilmente giunta a quella della *cibernetica*, dal nome della disciplina che studia l'elaborazione e la trasmissione delle informazioni fra sistemi complessi (organismi viventi, macchine o strutture organizzative). L'interesse degli scienziati moderni, più che all'*hardware* ed ai programmi informatici, si rivolge dunque alle *informazioni* oggetto di trasferimento e trattamento, nonché alle *modalità* secondo le quali queste attività possono svolgersi. Invero la maggior parte degli obiettivi della cibernetica (tra i quali figura, ad esempio, l'installazione di dispositivi nel corpo umano che simulino il comportamento del cervello e agevolino la trasmissione delle informazioni), ancorché siano stati parzialmente conseguiti (non senza gravi implicazioni bioetiche), necessitano ancora di perfezionamento.

Diversamente sembra potersi ritenere pienamente realizzato lo sfruttamento del *cyberspazio*, ovverosia il *non-luogo* virtuale dematerializzato, detemporalizzato e depersonalizzato in cui le informazioni giungono al destinatario in tempo reale, ovunque egli si trovi fisicamente. In proposito si pensi all'importanza assunta - nella vita quotidiana di ognuno di noi - da *Internet* e dai *social networks* (specie con il *lockdown* da COVID-19), connotati da meccanismi di interazione che hanno sostituito integralmente (o quantomeno parzialmente) l'instaurazione dei rapporti interumani reali.

Nel primo capitolo di questo elaborato si sono indagate le implicazioni giuspenalistiche della cibernetica.

Sul punto si è preliminarmente osservato come alcuni Stati abbiano cercato di assoggettare al loro potere il *cyberspace*, sinanco progettando la realizzazione di reti internet domestiche (si pensi alla creazione di «*Runet*» da parte della Federazione Russa), che consentano di sganciarsi dalla rete internet globale, la quale non può essere controllata a causa delle infinite interconnessioni che la connotano. Tuttavia la non equiparabilità degli *utenti* della rete internet ad un *popolo* e l'impossibilità di qualificare il *cyberspace* alla stregua di un *territorio perimetrabile* escludono che, nella dimensione cibernetica, possa operare il paradigma tradizionale della *Sovranità*.

La mancanza di un controllo nel cyberspazio ha favorito la diffusione dei *cybercrimes*. Trattasi dei reati commessi nello spazio cibernetico, che si differenziano ontologicamente dai *computer crimes* (sia sotto il profilo oggettivo che soggettivo), senza richiedere, tra gli elementi essenziali del

fatto tipico, un *computer* o un sistema informatico (che non sono l'oggetto materiale del reato né il bene giuridico da tutelare sotto il profilo dell'integrità). La crisi innescata dalla cibernetica, inoltre, interessa anche le categorie del diritto penale tradizionalmente impiegate per individuare il *tempus* ed il *locus commissi delicti*, che non possono applicarsi nel *cyberspace*, siccome privo delle coordinate spazio-temporali del mondo fisico.

I *cybercrimes* si distinguono dai *computer crimes* anche per il bene giuridico offeso, che non è riconducibile all'*inviolabilità del domicilio* (artt. 615-*ter*, 615-*quater*, 615-*quinquies* c.p.), né a quella dei *segreti* (617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies* c.p.), né, infine, al *patrimonio* (artt. 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies*, 640-*ter* c.p.), giacché gli utenti del cyberspazio – che ormai godono di un *habeas data* - meritano adeguati livelli di *autodeterminazione informativa*, *sicurezza* e *riservatezza informatiche*.

Il rinnovato interesse della scienza per la cibernetica ed i beni giuridici emersi in relazione ad essa impongono di elaborare una categoria di reati che, dogmaticamente, tenga conto dei predetti profili critici (in particolare di quelli legati al *cyberspace*), con la costruzione di nuove fattispecie incriminatrici irrinunciabilmente conformi ai principi del diritto penale costituzionale.

La seconda parte del primo capitolo è dedicata al *cyberterrorismo*, ovverosia il *cybercrime* politico che presenta il maggior grado di disvalore penale e rispetto al quale emergono vividamente tutte le suesposte criticità.

Trattasi del fenomeno frutto della commistione fra *reati cibernetici* e *terrorismo*, che tuttavia - diversamente dall'impostazione dalla dottrina tradizionale - non può disciplinarsi attraverso la mera giustapposizione delle norme relative alle suddette due categorie di reati. Siffatta semplicistica scelta regolatrice è frutto di definizioni del fenomeno approssimative e scarsamente connotate sotto il profilo giuridico. Queste, invero, concentrandosi sugli aspetti tecnici e scientifici, tralasciano di approfondire gli elementi essenziali dei reati di terrorismo comune. Il nostro ordinamento, nella perdurante mancanza di una definizione trasversalmente condivisa di *condotte terroristiche*, si limita a fornirne una che - a tacere dei profili di indeterminatezza - ne valorizza solo gli aspetti psicologici e precisamente finalistici (art. 270-*sexies* c.p.).

Nel primo capitolo, dunque, ci si prefigge di indagare quali siano le caratteristiche del terrorismo comune sotto il profilo oggettivo e soggettivo - soffermandosi in particolare sui concetti di «*natura*» e «*contesto*» - al fine di elaborare una definizione giuridica del cyberterrorismo.

Per quanto riguarda il contrasto del fenomeno, diritto europeo e diritto nazionale hanno optato per strategie che, pur accomunate dalla medesima *ratio preventiva*, divergono profondamente quanto agli strumenti attuativi.

Il diritto eurounitario, ancorché attualmente non preveda una disciplina autonoma e sistematica del cyberterrorismo (termine che, differentemente dalle fonti statunitensi, quelle europee non utilizzano), ha dimostrato grande attenzione per il tema.

Attesa la frammentarietà e disorganicità delle fonti rilevanti in materia, nel secondo capitolo dell'elaborato si è ritenuto di procedere ad un esame interdisciplinare degli atti di diritto derivato che si occupano di *infrastrutture critiche* (direttiva 2008/114/CE), *sistemi di informazione* (2013/40/UE), *sicurezza delle reti e dei sistemi informativi* (direttiva UE 2016/1148), *cybersecurity* e *cyberresilience* (regolamento 2019/881 c.d. *Cybersecurity Act*).

Ebbene, nell'arco di quindici anni il legislatore europeo si è assiduamente occupato della cibernetica, elaborando definizioni indispensabili per comprendere la materia (ad esempio quella di *infrastruttura critica dello Stato*); ha evidenziato l'emergere di nuovi beni giuridici da tutelare (in particolare la *cybersicurezza*); ha predisposto strategie per prevenire i reati cibernetici, individuando nella *cyberresilieza* il loro principio ispiratore ed attribuendo nuove prerogative all'Agenzia europea per la cybersicurezza (ENISA). Infine con la direttiva 2017/541 ed il regolamento 2021/784 è stato introdotto il concetto di *terrorismo online*, richiedendo agli Stati membri di prevedere *fattispecie di reato* e *misure di prevenzione* (precipuamente positive) per il contrasto preventivo del fenomeno.

Nel terzo capitolo si sono esaminati gli strumenti, tra quelli noti all'ordinamento italiano, che possono essere impiegati per la prevenzione del cyberterrorismo, anche alla luce dell'attuazione delle prescrizioni europee. L'assenza di una disciplina dei *cybercrimes* impone di concentrarsi sullo strumentario predisposto per contrastare i reati di terrorismo comune.

La strategia italiana in materia è stata finora contraddistinta dall'iperproduzione di fattispecie delittuose, introdotte di volta in volta all'indomani degli attentatati terroristici che - a partire dal *Nine Eleven* - hanno insanguinato l'Europa occidentale negli ultimi decenni, connotate da una valenza simbolica più che da una reale efficacia preventiva e repressiva.

Tra queste fattispecie figura un'unica previsione espressamente dedicata alle condotte terroristiche compiute con i mezzi informatici, ovverosia l'aggravante per l'*addestramento ad attività con finalità di terrorismo anche internazionale commesso attraverso strumenti informatici o telematici* (art. 270-*quinquies*, co. 2, c.p.).

Più in generale la legislazione italiana contro il terrorismo prevede fattispecie delittuose prevenzionistiche connotate dall'anticipazione della soglia della rilevanza penale - sinanco anteriormente al tentativo punibile (art. 56 c.p.) - mediante tecniche di incriminazione frutto dell'accostamento abnorme di istituti del diritto penale quali, ad esempio, la struttura del reato di pericolo ed il dolo specifico. In ogni caso, l'impiego della pena - che per definizione deve applicarsi all'esito di un processo che abbia accertato la responsabilità del reo - in funzione eminentemente

specialpreventiva ha l'effetto di generare una risposta sostanzialmente inefficace rispetto alle nuove condotte cyberterroristiche, con frizioni rispetto ai principi costituzionali (in particolare quelli di *determinatezza* ed *offensività*).

Il principale obiettivo di questo lavoro, dunque, consiste nel ricercare degli *strumenti alternativi alla pena*, che, intervenendo *ante delictum* sugli elementi della *natura* e del *contesto* delle condotte cyberterroristiche, ne azzerino l'idoneità offensiva e dissuadano i soggetti agenti dal perseguimento delle finalità tipizzate dall'art. 270-*sexies* c.p.

La disciplina delle misure di prevenzione, oggi regolata dal d.lgs. 159/2011 (c.d. *Codice delle leggi antimafia e delle misure di prevenzione*), offre interessanti spunti di riflessione sul tema. Tuttavia la sua applicabilità alla materia del cyberterrorismo richiede un adeguamento – *de iure condendo* - in punto di *categorie soggettive* e *pericolosità sociale*, alla luce dei principi elaborati dalla Corte Costituzionale italiana (Cass., SS.UU., sent. 24.4.2015, n. 17325), all'esito del "dialogo mediato" recentemente intrattenuto con la Corte Europea dei Diritti dell'Uomo (CEDU, Grande Camera, sent. 23.2.2017, De Tommaso c. Italia - ricorso n. 43395/09).

La ricerca è stata condotta attraverso un attento vaglio delle più recenti fonti dottrinali e giurisprudenziali in materia. La dimensione transnazionale (*rectius* deterritorializzata) del cyberterrorismo ha imposto di esaminare il fenomeno anche in un'ottica comparatistica, attingendo ai contributi di giuristi statunitensi, dal momento che l'ordinamento nordamericano si occupa di *deterrence and prevention of cyberterrorism* almeno sin dal 2001 (sec. 814, Patriot Act del 26.10.2001). L'esame delle fonti europee rilevanti in materia – sebbene, sotto il profilo formale, non prevedano l'impiego del termine cyberterrorismo - è stato indispensabile al fine di reperire le definizioni per comprendere la portata del fenomeno criminoso ed elaborare la strategia per il suo contrasto preventivo.

CAPITOLO I

Definizione e inquadramento giuridico del cyberterrorismo: l'inadeguatezza delle categorie tradizionali del diritto penale

SOMMARIO: 1. La cibernetica e gli effetti "rivoluzionari" delle tecnologie dell'informazione e della comunicazione sui rapporti interumani. – 2. Il cyberspazio: origine, definizione e caratteri giuridicamente rilevanti. – 3. Dallo Stato territoriale al cyberspazio: la crisi della sovranità. - 4. Gli illeciti penali nel cyberspazio: dai reati informatici ai reati cibernetici. – 4.1. Quale *locus commissi delicti* nel cyberspazio? La risposta della giurisprudenza. – 4.2. La ricerca del bene giuridico comune ai reati cibernetici: l'incompatibilità fra cyberspazio e inviolabilità del domicilio. - 4.3. L'evoluzione della tutela degli interessi giuridici connessi alle tecnologie dell'informazione nel diritto europeo: la cybersicurezza come bene giuridico offeso dai reati cibernetici. – 5. Il cyberterrorismo: nascita del concetto e tentativi definitori. – 6. Il terrorismo: etimologia ed evoluzione storica. - 6.1. La definizione europea di reato terroristico. - 6.2. La definizione italiana di condotte con finalità di terrorismo (art. 270-*sexies* c.p.) – 6.3. I presupposti oggettivi della finalità di terrorismo individuati dalla giurisprudenza di legittimità. – 6.4. Le tecniche incriminatrici anticipatorie della soglia della punibilità impiegate nella tipizzazione dei reati terroristici. - 7. Osservazioni conclusive.

1. La cibernetica e gli effetti "rivoluzionari" delle tecnologie dell'informazione e della comunicazione sui rapporti interumani

La diffusione delle nuove tecnologie per lo scambio di informazioni ha assunto, almeno a partire dalla metà dello scorso secolo, il ruolo di bussola e volano dello sviluppo umano. Il fenomeno, che dapprima ha interessato peculiarmente il sistema produttivo post-industriale, ha da sùbito suscitato

l'attenzione della sociologia e dell'economia, le quali, in proposito, hanno coniato l'espressione «rivoluzione informatica»[1]. Successivamente il termine è invalso per descrivere lo sviluppo delle attività che pertengono al processo di ricerca, raccolta e scambio di informazioni mediante nuovi strumenti tecnologici.

La rivoluzione informatica - protrattasi per tutto il quarantennio compreso fra gli anni '50 e i '90 del XX secolo - ha conosciuto il suo apice con la nascita del *World Wide Web* e perdura tutt'oggi, sebbene con il nuovo millennio si sia assistito ad un mutamento sia del suo oggetto sia del suo ambito applicativo.

Più precisamente, sotto il primo profilo, si osserva come attualmente la ricerca scientifica, funzionale all'ideazione di tecnologie, non si limiti più allo studio delle attività di raccolta e scambio delle informazioni. Essa pare piuttosto indirizzarsi verso un esame unitario dei processi che riguardano la comunicazione nell'uomo e nella macchina, con un fine ambizioso: conformare la seconda al primo, financo munendola di meccanismi tali da riprodurne le peculiari capacità cognitive e comunicative[2]. Il mutamento registratosi trova altresì ragione nella maturata consapevolezza che il trasferimento delle informazioni avviene in un'apposita dimensione avente natura virtuale: il cyber-spazio. Questo si configura come una realtà depersonalizzata, deterritorializzata e dematerializzata,

---

[1] Il concetto di «rivoluzione informatica» è apparso per la prima volta nel saggio *Information Revolution* (1974) dell'economista D. M. Lamberton, che impiegò il termine per evidenziare come la portata innovativa della tecnologia dell'informazione, rispetto alla società, fosse equiparabile a quella delle rivoluzioni agricola ed industriale. Invero, già a partire dagli anni '40 del XX secolo, le scienze applicate avevano iniziato a dedicarsi allo studio dei legami intercorrenti fra tecnologia e comunicazione. In particolare lo statistico N. Wiener (1894 – 1968) si occupò di definire il campo di indagine della *cibernetica* nel saggio *The human use of human beings* (1953). Sul concetto di «rivoluzione informatica» si veda anche J. R. BENIGER, *The Control Revolution: Technological and Economic Origins of the Information Society*, Harvard University Press, 1986, pp. 291 e ss.

[2] F. PARENTE, *Sistemi cibernetici, autoapprendimento integrale e intelligenza connettiva*, in *Annali del Dipartimento Jonico dell'Università degli Studi di Bari*, EDJzioniSGE, 2018, p. 267; N. WIENER, *The human use of human beings*, Houghton Mifflin, 1953, trad. it. a cura di D. PERSIANI, *Introduzione alla cibernetica*, Bollati e Beringhieri, 1997, pp. 23 e ss. Sul punto è appena il caso di ricordare che la questione non è più confinabile entro gli stringenti limiti della fantascienza, atteso – solo a titolo esemplificativo - il progetto elaborato dall'imprenditore Elon Musk, che intende sperimentare l'installazione di *microchip* nel cervello umano in funzione di interfaccia con i *computers*. Il progetto è consultabile al *link* dell'azienda di Musk: *https://neuralink.com/approach/*.

per la cui definizione non possono più impiegarsi le categorie tradizionali che connotano lo spazio fisico[3].

Con riguardo al mutamento dell'ambito applicativo, invece, si registra un consistente ampliamento del novero dei settori in cui trovano applicazione le risultanze dell'attività di ricerca scientifica. Queste, differentemente da quanto accaduto nel primo periodo della rivoluzione, oggi non interessano più il solo settore produttivo, ricevendo, anche grazie ai costi sempre più contenuti, una diffusione massiva.

Alla luce di detti mutamenti, i più autorevoli commentatori in materia hanno condivisibilmente sostenuto che la rivoluzione informatica ha subito una virata che - valorizzando il rinnovato orientamento teleologico dimostrato dalla ricerca scientifica – è stata definita «cibernetica»[4].

Il termine viene impiegato per indicare l'insieme delle tecnologie volte all'*elaborazione e trasmissione dell'informazione fra sistemi complessi*, tra i quali sono ricompresi organismi viventi, macchine e strutture organizzative. L'obiettivo più ambizioso della cibernetica consiste nella creazione di macchine che siano in grado di simulare i comportamenti del cervello umano[5].

La parola «cibernetica» deriverebbe dalla radice sanscrita *kubera*-, che, come risulta da attestazioni risalenti al IX secolo a.C., era impiegata per

---

[3] P. LEVY, *Il virtuale*, Raffaello Cortina, 1997, pp. 9-14, nonché A. F. VIGNERI, *Cyberterrorismo: realtà o finzione? Profili problematici di definizione e contrasto*, 3.9.2018, in *Opinio Juris,* pp. 8 e ss.

[4] R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *Dir. Pen. Comp*., 20.9.2012, pp. 1-13 e in particolare il paragrafo *Il "nuovo millennio" ed il passaggio dal computer crime al cybercrime*, pp. 3-5; F. RESTA, *Virtualità del crimine. Dai reati informatici ai cybercrimes*, in *L'informatica del diritto*, in *Giur. Merit.*, 11/2006, pp. 102 e ss.

[5] N. WIENER, *Cybernetics, or control and communication in the animal and the machine,* The MIT Press*,* 1948*,* pp. 11 e ss. Il connotato cibernetico della virata della rivoluzione informatica trova conferma nella definizione fornita da Wiener, secondo il quale la cibernetica - di cui l'autore è considerato padre fondatore - è: «the study of control and communication in the animal and the machine»; conforme la voce *Cibernetica*, in Treccani - *Enciclopedia on line*, *https : / / www . treccani . it / enciclopedia / cibernetica _ res - 8f9c1cae - 87e7 - 11dc - 8e9d 0016357eee51 _ % 28Enciclopedia – Italiana % 29 /.*

significare il concetto del timone delle imbarcazioni[6]. Il termine greco *kybernetes* (κυβερνήτης), poi, la cui esistenza è testimoniata da fonti di epoca classica (480-323 a.C.), era usato con il significato di *timoniere* o *pilota*, nonché, in senso figurato, con quello di «conduttore di popoli»[7].

Ebbene, alla luce delle considerazioni sopra svolte in relazione alle finalità della scienza cibernetica, pare che questa, oggi più che mai, sia "guida" per l'uomo, in quanto si dimostra capace di condizionare (*rectius* orientare) i settori più rilevanti della sua esistenza. Oggi le tecnologie cibernetiche detengono un ruolo indispensabile - in alcuni casi gioco forza necessitato - nella vita quotidiana di tutte le persone, caratterizzandone, in modo più o meno consistente, almeno una parte dei rapporti sociali. Si tratta di una tendenza che, nell'ultimo decennio, ha subito una forte accelerazione - sino ad esasperarsi a causa della situazione creatasi per la pandemia da COVID19 - a seguito della comparsa dei *social networks* e del loro uso quotidiano. Tali strumenti emblematizzano la vocazione della cibernetica, dal momento che consentono a ciascun utente - anche nel totale anonimato o, peggio, impiegando false identità - di "aggiungere agli amici" persone in realtà sconosciute, di comunicare i propri stati emotivi e i propri pensieri in tempo reale (ad esempio con l'apposita funzionalità di *Facebook* "A cosa stai pensando"), di condividere idee ed opinioni attraverso *reactions*, di pubblicare *posts*, foto o *stories*, magari con finalità pubblicitarie.

Sul punto si pensi alle profonde modifiche registratesi in materia di comunicazione politica, atteso il sistematico impiego dei *social networks*, da parte delle Istituzioni, per interagire con gli elettori. E ciò non solo per compiere esternazioni e dichiarazioni che chiunque può liberamente commentare, ma anche per rendere note le scelte politiche assunte dal Governo, talvolta prima della pubblicazione del relativo atto. Alcuni partiti politici, poi, consentono ai propri iscritti di partecipare direttamente all'assunzione delle scelte politiche,

---

[6] A. F. VIGNERI, *Brevi considerazioni sulla natura e sulle caratteristiche dello spazio cibernetico*, in *SalvisJuribus*, 10.10.2019, disponibile al link: *http://www.salvisjuribus.it/brevi-considerazioni-sulla-natura-e-sulle-caratteristiche-dello-spazio-cibernetico/*.

[7] PLATONE (a cura di M. MIGLIORI), *Politico*, Bompiani, 2001, p. 25.

esprimendo il proprio voto su apposite piattaforme. In senso antidemocratico, invece, meritano censura gli usi distorsivi dei *social networks*, tra i quali figura la profilazione degli utenti, al fine di condizionarne indirettamente le scelte politiche durante la campagna elettorale, come sarebbe accaduto nei casi *Datagate* e *Russiagate*[8].

Altro settore in cui le *communication technologies* stanno riscontrando crescente impiego è la finanza, con particolare riguardo agli strumenti di pagamento ed investimento. In relazione a questa tematica, particolare interesse suscita la diffusione della cosiddetta *criptovaluta* (o *criptomoneta*), consistente in una rappresentazione digitale di valore su base crittografica, impiegata come mezzo di scambio o detenuta a scopo di investimento, il cui utilizzo e visibilità sono condizionati al possesso di appositi codici informatici o chiavi d'accesso. Le caratteristiche del sistema in cui tali strumenti finanziari vengono utilizzati (connotato dalla totale assenza di un'autorità centrale che esplichi una funzione regolatoria e da un modello di scambio *peer to peer*) sono chiaro esempio della depersonalizzazione dei sistemi cibernetici[9].

---

[8] Per un esame dei profili giuridici dei casi *Datagate* e *Russigate* si rinvia a M. BARTOLOMÉ, *Cybersecurity in the second decade of the Twenty-First Century*, in AA.VV., J. CAYÓN PEÑA (a cura di), *Security and defence: ethical and legal challenges in the face of current conflicts*, Springer, 2022, pp. 57 e ss. In particolare con «Datagate» si indica lo scandalo scoppiato negli Stati Uniti nel 2013 a seguito della rivelazione di alcuni documenti da parte di Edward Snowden (*ex* funzionario dell'Agenzia per la Sicurezza Nazionale statunitense – NSA), i quali proverebbero l'attuazione, da parte dell'*intelligence* statunitense, del programma di sorveglianza di massa (a livello mondiale) denominato ECHELON. Questo consisterebbe in un sistema globale di intercettazione di comunicazioni private e commerciali, con il quale sarebbero stati carpiti dati ed informazioni relative a privati cittadini ed a Istituzioni sia statunitensi che straniere. «Russiagate», invece, è il termine giornalistico impiegato per indicare le presunte ingerenze esercitate dalla Federazione Russa nelle elezioni presidenziali statunitensi del 2016, vinte da Donald Trump. Il procedimento penale promosso negli Stati Uniti nel 2017 (Procuratore speciale Robert Muller), è volto ad accertare le responsabilità del Governo e dell'*Intelligence* russi e vede alcuni funzionari dei servizi segreti militari russi imputati di *spionaggio a favore di potenza straniera*.

[9] G. P. ACCINNI, *Cybersecurity e criptovalute. Profili di rilevanza penale dopo la Quinta Direttiva*, in *Sist. Pen*., 5/2020, 15.5.2020, pp. 211 e ss.

2. Il cyberspazio: origine, definizione e caratteri giuridicamente rilevanti

Tra gli elementi che caratterizzano la rivoluzione cibernetica vi è la dimensione virtuale in cui le informazioni vengono trasferite, ovverosia il cyberspazio (o *cyberspace*), di cui si è già fatto cenno. Attesa l'importanza di tale elemento, che attualmente resta sprovvisto di una definizione trasversalmente condivisa, si ritiene imprescindibile indagarne natura e caratteri.

Muovendo da considerazioni di ordine generale, è possibile osservare come il prefisso «*cyber-*» abbia la funzione di evidenziare il collegamento sussistente fra lo spazio virtuale e la natura cibernetica delle informazioni ivi circolanti, evidenziando la differenza fra il primo e lo spazio fisico, in cui prende luogo la condotta connotata da materialità.

Quanto all'origine, invece, il termine «*cyberspace*» (in italiano cyberspazio o spazio cibernetico) è stato coniato dallo scrittore William Gibson ed è apparso per la prima volta nel suo romanzo intitolato *Burning Chrome* del 1982[10]. Tuttavia, solo nel successivo romanzo intitolato *Neuromancer* del 1984, l'autore ne ha fornito la seguente definizione: «allucinazione vissuta consensualmente, ogni giorno, da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici, una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano»[11]. La definizione - sebbene scevra, come prevedibile, di profili giuridicamente rilevanti – presenta due aspetti che dovrebbero attirare l'attenzione del giurista. Il primo, invero piuttosto inquietante, consiste nelle vittime dell'allucinazione, le quali, secondo Gibson, sarebbero gli *operatori legali* di ogni nazione. Alla luce di un esame *ex post*, quanto sostenuto dall'autore si rivela a dir poco profetico, attese le difficoltà incontrate dal giurista moderno (a qualunque ordinamento egli

[10] W. GIBSON, *Burning Chrome*, Harper Collins, 2003.
[11] W. GIBSON, *Neuromancer*, Berkley Publishing, 1989, p. 128.

appartenga) nell'inquadrare giuridicamente il *cyberspazio*. Le principali difficoltà sono dovute all'incompatibilità delle categorie tradizionali del diritto penale – peculiarmente quelle impiegate per determinare la collocazione spaziale e temporale del fatto – rispetto alla natura virtuale (e comunque non fisica) della dimensione cibernetica, con conseguente ingenerazione di uno stato di disorientamento nel giurista. Il secondo aspetto della definizione, invece, riguarda la consensualità dell'«allucinazione». Questa, infatti, per esistere, richiede come presupposto il consenso degli utenti che se ne avvalgono, prescindendo da qualsiasi regolamentazione normativa, tanto da presentarsi come un fenomeno originariamente *a-nomico*[12].

Ad ogni modo il primo tentativo definitorio giuridicamente rilevante del concetto di *cyberspace* risale al 2009, quando un gruppo di venti giuristi - sotto il coordinamento del Prof. M. N. Schmitt[13] -, accogliendo l'invito del *Centro di eccellenza per la difesa cibernetica* della NATO, avviava uno studio volto ad indagare i rapporti sussistenti fra diritto internazionale ed operazioni cibernetiche penalmente rilevanti[14]. In particolare, l'obbiettivo del gruppo di lavoro consisteva nell'elaborazione di linee guida circa l'applicabilità delle categorie del diritto internazionale al *cyber-warfare*, nonché nella predisposizione di un primo *corpus* legislativo in materia di *cyber-operations*. I risultati della ricerca sono stati

---

[12] Sul carattere anomico del *cyberspace* L. PASCULLI, *The Global Causes of Cybercrime and State Responsibilities. Towards an Integrated Interdisciplinary Theory*, in *Journal of Ethics and Legal Technologies*, Vol. 2, 4/2020, pp. 5 e ss.; G. B. MCBEATH, S. A. WEBB, *Imagining cities*, Routledge, 2018, pp. 249 e ss.

[13] Preside del Dipartimento di Diritto Internazionale presso lo *United States Naval War College* di Newport, Professore di diritto internazionale umanitario presso la *Durham University*, nonché ex decano dell'Istituto per gli studi sulla sicurezza dell'Unione europea (EUISS).

[14] La necessità di avviare i lavori per approntare una regolamentazione a livello internazionale delle attività cibernetiche sorgeva già nel 2007, a seguito dell'attacco informatico sferrato dalla Russia ai danni dell'Estonia ed avente come oggetto materiale alcuni sistemi informatici governativi e alcune infrastrutture informatiche anche finanziarie del Paese. Tale avvenimento viene riconosciuto come il primo attacco con effetti cibernetici commesso da uno Stato ai danni di un altro, tanto che i governi dell'epoca si dimostrarono concordi nel ritenere che esso potesse legittimare l'applicazione dell'art. 5 del Patto Atlantico. Al fine di sviluppare la cooperazione fra gli Stati membri nel settore della difesa cibernetica, venne quindi fondato il NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), con sede a Tallinn.

raccolti nei cosiddetti Manuali di Tallinn, che, nonostante la loro rilevanza, restano tuttora un'opera priva di valore normativo vincolante[15].

In particolare, nel glossario del primo dei due manuali, i giuristi interpellati hanno offerto la seguente definizione di *cyberspace*: «ambiente formato da componenti fisici, caratterizzati dall'uso del computer, e da uno spettro elettromagnetico per memorizzare, modificare e scambiare dati tramite reti di computer»[16].

Concordemente a detta definizione, il *cyberspace* avrebbe dunque *natura ibrida*, componendosi di una *parte fisica* e di una *parte non fisica*.

La prima consisterebbe nei *devices* informatici e, più in generale, in tutti i dispositivi *hardware* (a partire dai fili e dai cavi per l'alimentazione elettrica) –

---

[15] Il primo Manuale di Tallinn è stato pubblicato nel 2013 per la *Cambridge University Press*, con il titolo *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Il secondo, invece, che rappresenta un aggiornamento del precedente, è stato pubblicato nel 2017 per la stessa casa editrice, con il titolo *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Come emerge dal titolo, il secondo manuale non è dedicato esclusivamente alla disciplina del *Cyberwarfare*, bensì, più generalmente, a quelle di tutte le *cyberoperations*. La struttura del manuale del 2017 (che ricalca quella del precedente) si articola nell'enunciazione di novantacinque regole, che, conformemente al diritto consuetudinario internazionale, predispongono una disciplina del *cyberspace*. La prima parte del manuale è dedicata al diritto internazionale della sicurezza cibernetica, mentre la seconda al diritto dei conflitti armati cibernetici. La prima parte è a sua volta ripartita in sette capitoli. Il primo contiene le sezioni riguardanti la *Sovranità*, la *giurisdizione*, il *controllo* e la *responsabilità dello Stato*; il secondo riguarda l'uso della forza e contiene le sezioni relative al *divieto dell'uso della forza*, alla *legittima difesa* e alle *azioni delle organizzazioni internazionali*. I capitoli terzo e quarto riguardano rispettivamente il *diritto dei conflitti armati* e la *condotta da serbare nel corso delle ostilità*. Il quinto tratta di *particolari categorie di persone ed attività* (ad esempio personale sanitario e religioso, unità mediche e trasporti, personale delle Nazioni Unite, detenuti, minori, giornalisti). Il capitolo sesto è dedicato all'*occupazione da parte di Stati stranieri*, mentre il settimo è dedicato alla *neutralità*. Per un esame critico delle tematiche affrontate nel secondo Manuale di Tallinn E. TALBOT, E. JENSEN, *The Tallinn Manual 2.0: Highlights and Insights*, in *Georgetown Journal of International Law*, Vol. 48, 2017, p. 735-778; W.H. VON HEINEGG, *Chapter 1: The Tallinn Manual and International Cyber Security Law*, in *Yearbook of International Humanitarian Law*, vol. 15, 2012, pp. 3-18; Y. SHANY, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, in *The American Journal of International Law*, vol. 112, no. 4, 2018, pp. 583-657.

[16] M. N. SCHMITT, *Tallinn Manual on the International Law applicable to Cyber Warfare*, Cambridge University Press, 2013, p. 258, in particolare la voce «Cyberspace» del *Glossary*, in cui si legge: «The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks».

dovendo oggi ricomprendersi, attraverso un procedimento analogico, non solo i *computers*, ma anche tutti gli altri strumenti diffusisi sul mercato grazie allo sviluppo tecnologico (come, ad esempio, *smartphone* e *ipad*) - mediante i quali è possibile accedere alla rete, per lo scambio di dati ed informazioni.

La seconda parte, invece, corrisponderebbe allo spettro elettromagnetico, non percettibile sensorialmente, in cui avviene lo scambio ed il trasferimento virtuale di dati ed informazioni.

Tale prima definizione esprime dunque una *concezione bipartita* di *cyberspace*, che rappresenta il nucleo fondante delle teoriche posteriormente elaborate in materia, le quali, perlopiù, hanno proceduto a completarla, aggiungendovi ulteriori elementi.

Un successivo tentativo definitorio è stato esperito da Shmuel Even e David Siman-Tov, che hanno formulato una definizione di *cyberspace* fondata su una *concezione tripartita*, articolata come segue:

- *the human layer*, ovverosia l'insieme degli utenti che, attraverso *accounts*, si avvalgono consapevolmente dei sistemi cibernetici per il trasferimento delle informazioni;
- *the logical layer*, ovverosia i *software* e, più in generale, tutti i sistemi privi di materialità in cui viaggiano le informazioni;
- *the physical layer*, ovverosia le infrastrutture e le apparecchiature fisiche, attraverso le quali l'utente può accedere al *cyberspace*[17].

La teoria tripartita si dimostra maggiormente condivisibile rispetto alla precedente. Infatti l'introduzione della terza "componente umana" - oltre a rendere la definizione più completa - riconduce il *cyberspace* entro il novero dei fatti umani. Tale osservazione consente di fugare ogni dubbio circa il rilievo giuspenalistico del *cyberspace* – dal momento che, come noto, il diritto penale è per definizione il diritto del fatto umano – e, conseguentemente, di negarne il carattere anomico[18].

---

[17] S. EVEN, D. SIMAN-TOV, *Cyber Warfare: Concepts and Strategic Trends*, Memorandum 117, The Institute for National Security Studies, 2012, pp. 10-11.

[18] L. PASCULLI, *op. cit.*, pp. 5 e ss.

Infine, per completezza, si ritiene opportuno segnalare un ulteriore orientamento dottrinale, secondo il quale la struttura del *cyberspace* sarebbe addirittura quadripartita. Il quarto elemento costitutivo - da aggiungere ad *physical*, *logical* e *human layer* - sarebbe rappresentato dagli stessi dati e informazioni trasferite attraverso il *cyberspace*[19]. Tuttavia tale impostazione non pare condivisibile, dal momento che il cyber-spazio ben può esistere a prescindere dalla presenza di informazioni in esso circolanti, quale scenario ove porre in essere condotte, le quali - come si dirà - possono avere rilevanza penale.

3. Dallo Stato territoriale al cyberspazio: la crisi della sovranità

Il riconoscimento della rilevanza giuridica dello spazio cibernetico ha suscitato l'interesse di alcuni Stati - accomunati da regimi politici illiberali ed autoritaristici – in ordine al controllo di sue porzioni.

In particolare la Russia, con la legge 1.5.2019, n. 90-FZ (c.d. *legge sull'internet sovrano*), ha previsto la realizzazione, in tempi brevi, di un sistema nazionale di sviluppo e gestione centralizzata del traffico internet, denominato *RuNet*[20].

---

[19] D. CLARK, *Characterizing Cyberspace: Past, Present, and Future*, in *MIT Review*, 12.3.2010, pp. 1-18; A. KLIMBURG, P. MIRTL, *Cyberspace and Governance - A Primer*, in *Austrian Institute for International Affairs* (Oiip), 9/2012, disponibile al *link*: *http : / / www . oiip . ac . at / publikationen / arbeitspapiere / publikationen – detail / article / 9 2 / cyberspace – and – governance – a – primer . html.* Per quanto riguarda la dottrina italiana, invece, U. GORI, *Lo spazio cibernetico e la sicurezza nazionale. Le nuove minacce cyber*, in *Lo spazio cibernetico tra esigenze di sicurezza nazionale e tutela delle libertà individuali*, supplemento al n. 6/2014 di *Informazioni della Difesa*, p. 8, in l'autore ritiene che lo spazio cibernetico consista in un sistema a quattro strati con funzioni differenziate, sebbene tutte ugualmente importanti o necessarie. Tali strati sono: i *fondamenti e le strutture fisiche*; i *blocchi logici che rendono possibili i vari servizi*; il *contenuto di informazioni inserito, trasmesso e trasformato*; gli *attori che interagiscono in questa arena in ruoli diversi*.

[20] La legge 1 maggio 2019, n. 90-FZ (entrata in vigore il 1 novembre 2019) reca modifiche alla legge federale sulle comunicazioni e alla legge federale sull'informazione, le tecnologie dell'informazione e la protezione dell'informazione (testo al link: *https://rg.ru/documents/2019/05/07/fz90-dok.html*).

Nella pratica la legge federale, il cui obiettivo ultimo è sganciare in modo assoluto e definitivo la Federazione Russa dalla rete internet globale, prescrive: l'iscrizione dei fornitori nazionali di servizi di telecomunicazione in un apposito registro controllato dal Governo; l'adozione, da parte degli stessi, di apposite apparecchiature volte a consentire allo Stato di analizzare e filtrare direttamente le informazioni inviate da mittenti stranieri a destinatari russi; la gestione centralizzata di *RuNet* da parte del *Servizio federale per la supervisione nella sfera della connessione e comunicazione di massa* (facente capo al Governo)[21].

Il controllo del cyberspazio da parte dello Stato, al di là della pratica attuabilità del progetto russo, pone due problematiche. Da un alto bisogna interrogarsi se sia possibile perimetrare lo spazio cibernetico, il quale - per sua natura - è deterritorializzato. Dall'altro lato, invece, è necessario verificare se il *cyberspace* sia *tout court* assoggettabile al paradigma tradizionale della *sovranità* statuale.

Sul punto giova osservare che la concezione tripartita del cyberspazio (Even e Siman-Tov) presenti innegabili analogie con la struttura dello Stato moderno, quale organizzazione politica composta da un *popolo* stabilmente stanziato su un *territorio*, su cui viene esercitato un *potere sovrano* per il raggiungimento di fini di interesse comune. Infatti il complesso formato da *logical layer* e *physical layer* corrisponderebbe alla componente del *territorio*, dal momento che il primo attiene ad aspetti che potrebbero definirsi latamente geografici (quali lo spostamento virtuale delle informazioni e la collocazione dei *devices* utilizzati dagli utenti cibernetici). Lo *human layer*, invece, corrisponderebbe al *popolo*.

Diversamente, meno immediata risulterebbe l'individuazione di un elemento che, nel *cyberspace*, rappresentati la *sovranità*. Questa, secondo chi sostiene la tesi del rapporto analogico predetto, sarebbe componente sostanziale

---

[21] Per un dettagliato esame del sistema *RuNet* sotto il profilo tecnico e giuridico - nonché delle sue possibili ricadute politiche, culturali e sociali - si rinvia a N. KONRADOVA, *The rise of RuNet and the main stages of its History*, in AA.VV., S. DAVYDOV (a cura di), *Internet in Russia A Study of the Runet and Its Impact on Social Life,* Springer, 2020, pp. 39 e ss.

del ciber-spazio, accomunandolo direttamente allo Stato[22]. Anche a voler condividere questa tesi, si ritiene che i termini di estrinsecazione del potere sovrano nel *cyberspace* siano diversi. Infatti, mentre nel caso dello Stato la *sovranità* è esercitata nei confronti di un popolo che si trova in un determinato territorio, in quello dello spazio cibernetico essa si rivolge nei confronti degli utenti che utilizzano i sistemi *hardware* e *software* per lo scambio di dati ed informazioni. Pertanto è evidente che sostenere uno stretto rapporto analogico fra Stato e *cyberspace* - cercando di rinvenire, ad ogni costo, corrispondenze fra i rispettivi elementi costitutivi - comporta il rischio di ridurre il secondo ad un'ulteriore dimensione (priva di autonomia) di esercizio della sovranità statuale. In proposito si è parlato di un processo di *territorializzazione dello spazio virtuale*, che condurrebbe a descrivere il complesso formato da *Stato-sovranità-cyberspace* negli stessi termini di quello *Stato-sovranità-territorio*[23].

Altri autori hanno qualificato il fenomeno appena descritto come *alignment*. Più precisamente il termine viene impiegato per indicare il fenomeno sostanziantesi nel tentativo di ricondurre il cyber-spazio entro una forma che sia "riconoscibile" da parte dello Stato territoriale - e quindi compatibile con la sua struttura – mediante l'uso dei tradizionali criteri spazio-temporali. In questo senso l'*alignment* può assumere almeno tre diverse forme[24].

---

[22] A sostegno di questa tesi N. TSAGOURIAS, R. BUCHAN, *International Law and Cyber Space*, Cheltenham, 2015, pp. 19, in cui si legge: «the State can exercise its prescriptive and enforcement jurisdiction over cyberspace and over cyber activities on the basis of nationality and territoriality»; E. JENSEN, E. TALBOT, *Cyber Sovereignty: The Way Ahead*, in *Texas International Law Journal*, 2015, p. 275, in cui si legge: «as a matter of sovereignty, States have the right to develop their cyber capabilities according to their own desires and resources». Inoltre, a sostegno di questa tesi, si colloca anche quanto previsto dalla *rule* n. 1 del secondo Manuale di Tallinn, che recita: «The principle of sovereignty applies in cyberspace».

[23] Sul concetto della *territorializzazione* del *cyberspace* si veda U. GORI, *L'inarrestabile sviluppo delle armi cibernetiche*, in U. GORI, S. LISI (a cura di), *Cyber Warfare. Armi cibernetiche, sicurezza nazionale e difesa del buesiness*, Franco Angeli, 2014, pp. 11 e ss.; J. P. DARNIS, C. POLITO, *La Geopolitica del digitale*, Nuova cultura, 2019, p. 11.

[24] Sul concetto di *alignment* M. MUELLER, *Sovereignty and Cyberspace: Institutions and Internet governance*, 5th Annual Vincent and Elinor Ostrom Memorial Lecture, University of Indiana, 3.10.2018, pp. 3 e ss., disponibile al *link*: *https : / / dlc . dlib . indiana . edu / dlc / bitstream / handle / 10535 / 10410 / 5th – Ostrom - lecture DLC . pdf ? sequence = 1&isAllowed =*

Nella sua versione più rigida e restrittiva, esso si sostanzia in un controllo delle informazioni scambiate, filtrando – o, se necessario, addirittura bloccando – l'accesso ai servizi da parte di utenti appartenenti a Stati terzi, generalmente avvalendosi di un'apposita infrastruttura di telecomunicazioni facente capo allo Stato[25]. Una seconda forma di *alignment* consiste nel prevedere che i servizi – precipuamente quelli di *computer clouding* -, erogati dai fornitori del settore dell'informatica e delle telecomunicazioni, abbiano come destinatari esclusivamente i cittadini di un determinato Stato[26]. In altri casi, invece, l'*alignment* assume forme tali da incidere sotto profili di natura più propriamente economica. Invero alcuni Paesi si sono spinti a prevedere delle misure atte a scoraggiare l'erogazione e la fruizione, nel proprio territorio, di servizi finanziari cibernetici provenienti da fornitori stranieri. Altri Paesi, invece, hanno previsto restrizioni o, addirittura, divieti ad investimenti, da parte di Paesi terzi, a favore dei fornitori di servizi informatici operanti nel proprio territorio.

Come emerge dal raffronto appena operato tra le tre forme di *alignment*, queste presentano un denominatore comune sotto il profilo teleologico. Infatti ciascuna di esse mira, seppur con modalità diverse, a territorializzare il *cyberspace* o comunque a delimitarlo sulla base dei confini nazionali. Solo in questo modo si permetterebbe allo Stato di esercitare il potere sovrano sullo spazio cibernetico, identicamente a quanto avviene rispetto al territorio.

Tuttavia l'obbiettivo perseguito attraverso i diversi processi di territorializzazione si rivela utopico e logicamente contradditorio se letto alla luce della caratteristica che, senza paura di smentita, può ritenersi emblematica dello

---

y, in cui l'autore definisce l'*alignment* come: «an attempts to push global cyberspace into a shape recognizable to the territorial state. Alignment takes the following forms»

[25] M. MUELLER, *Ibidem*, pp. 3 e ss..

[26] M. MUELLER*, Ibidem*, pp. 3 e ss. In proposito si è parlato di «localizzazione dei servizi». Esempi di questa forma di *alignement* sono rappresentati dalla legislazione sulla sicurezza informatica del Vietnam e della Cina. Nel caso del primo Paese, il Ministero della pubblica sicurezza richiede a tutti i fornitori di servizi informatici stranieri di archiviare i dati dei cittadini esclusivamente nei *data center locali*. Il governo di Pechino, invece, ha deciso di limitare il funzionamento delle *infrastrutture critiche cibernetiche* dello Stato alla Cina continentale, imponendo rigidi requisiti di archiviazione dei dati agli operatori, che, anche in questo caso, possono archiviare i dati dei cittadini esclusivamente in *data centers* locali.

spazio cibernetico: l'*assenza di limitatezza*. Infatti, diversamente da quanto accade nel caso del territorio - inteso quale area geografica o, più in generale, come porzione di superficie terrestre - il *cyberspace*, per la sua stessa natura, non può essere ristretto entro dei confini. Una simile operazione finirebbe per vanificare il merito più grande dell'*Internet* - e oggi dei *social networks* - ovverosia la possibilità di scambiare in pochissimi secondi grandi quantitativi di informazioni tra utenti che si trovano a migliaia di chilometri di distanza.

Infine giova osservare che il riconoscimento della rilevanza giuridica – operata a livello internazionale - a domini sui quali gli Stati territoriali non esercitano la loro sovranità, consente di escludere la necessità che il *cyberspace* debba essere assoggettato al tradizionale paradigma del potere statuale. Tra questi domini figurano le *acque internazionali*, ovverosia quelle che si estendono oltre le dodici miglia dalla costa dello Stato. Rispetto a tale area marina, infatti, non trova applicazione il principio di territorialità per l'individuazione del *locus commissi delicti*[27].

In conclusione di paragrafo si può osservare come lo spazio cibernetico non possa essere assoggettato al potere sovrano degli Stati. Invero le definizioni del *cyberspace* elaborate dalla dottrina hanno evidenziato differenze ontologiche fra il trinomio *popolo-territorio-sovranità* e il trinomio *logical layer-physical layer-human layer*, tali da impedire di estendere al secondo il paradigma tradizionale della sovranità. In ogni caso la *regionalizzazione* dello spazio cibernetico, la quale è fisicamente impossibile (attesa la natura deterritorializzata dello stesso) se non nella forma di un distacco dalla rete internet globale, avrebbe l'effetto di frustrare le potenzialità ed i pregi della comunicazione cibernetica.

---

[27] Sul punto rileva ricordare quanto previsto dal Trattato internazionale sullo spazio extra-atmosferico del 27.1.1967, che al relativo art. 2 statuisce: «Lo spazio cosmico, inclusa la luna e gli altri corpi celesti, non è soggetto all'appropriazione nazionale attraverso la rivendicazione della sovranità […]».

4. Gli illeciti penali nel cyberspazio: dai reati informatici ai reati cibernetici

La svolta cibernetica della rivoluzione informatica ha favorito la diffusione su larga scala di *devices* informatici e dispositivi tecnologici, ormai irrinunciabili nella quotidianità di ogni persona, contribuendo innegabilmente a migliorare ogni settore della vita umana.

Tuttavia lo *spazio cibernetico* si è rivelato, per le sue peculiarità, terreno fertile per la manifestazione, secondo nuove modalità, di comportamenti già penalmente rilevanti e financo per l'integrazione di nuovi fatti di reato, dotati di propria autonomia. Questi illeciti vengono definiti *reati cibernetici* (o *cybercrimes*), per evidenziarne il legame consustanziale con il *cyberspace*.

Più in generale, giova osservare come ciascuna delle diverse fasi della rivoluzione tecnologica, iniziata negli anni '50 dello scorso secolo, sia stata connotata da peculiari manifestazioni criminali che, di volta in volta, hanno sfruttato, con abilità e rapidità, le potenzialità del momento.

La prima parte del suddetto processo innovatore è stato segnato dalla diffusione dei cosiddetti *reati informatici* (o *computer crimes*).

Il primo intervento per il contrasto di questi illeciti, registratosi a livello europeo, è rappresentato dalla Raccomandazione del Consiglio d'Europa del 9 settembre 1989, n. R (89)-9, relativa alla criminalità in rapporto all'*elaboratore informatico*[28], con la quale si è inteso promuovere una strategia comune contro i nuovi reati, suggerendo agli Stati membri dei criteri comuni secondo cui orientare le scelte di tutela penale in materia[29].

---

[28] Conseil de l'Europe, *Recommandation n. R(89)-9*, *sur la criminalité en relation avec l'ordinateur*. Per un esame critico dei contenuti della Raccomandazione si rinvia a C. LARINNI, *Garantismo europeista: un ossimoro? a proposito dell'accesso abusivo ad un sistema informatico o telematico (615-ter c.p.)*, in *DisCrimen*, 29.6.2020, pp. 9 e ss. Nella Raccomandazione si evidenzia la necessità di intervenire rapidamente contro il nuovo fenomeno della criminalità informatica - denunciandone il carattere transfrontaliero - con un rafforzamento delle politiche legislative nazionali in materia.

[29] Sul punto F. MAZZA, *Una nuova forma di criminalità economica: la pirateria informatica. Orientamenti dell'Unione Europea e strategie di contrasto, in Spunti critici in tema*

La Raccomandazione offre un'elencazione delle condotte rilevanti per l'integrazione dei reati informatici, ripartendole in due gruppi. Gli Stati membri sono tenuti a punire le condotte ricomprese nel primo gruppo, mentre sono liberi di scegliere se attribuire penale rilevanze a quelle appartenenti al secondo[30].

La Raccomandazione è stata recepita nell'ordinamento italiano a mezzo della legge del 23 dicembre 1993, n. 547, che ha introdotto complessivamente nove fattispecie delittuose comunemente definite *reati informatici*[31].

Sul punto, mancante una definizione normativa, vale la pena di soffermarsi sul concetto giuspenalistico di *computer crime*.

Con questa espressione si intende indicare ogni reato che presenti, fra gli elementi costitutivi della fattispecie astratta di riferimento, un *computer* - attraverso il quale sia possibile accedere alla rete - ed il relativo sistema informatico[32].

---

di nuove forme di criminalità, in AA.VV., *Spunti critici in tema di nuove forme di criminalità*, 2007, pp. 40 e ss.

[30] Le condotte informatiche appartenenti al primo gruppo, che potrebbe definirsi "obbligatorio", sono: il falso in documenti informatici, la frode informatica, il sabotaggio informatico, il danneggiamento di dati, l'intercettazione di comunicazioni informatiche, l'accesso abusivo a un sistema informatico e la violazione dei diritti di esclusiva su un programma informatico protetto. Nel secondo gruppo "facoltativo", invece, sono ricomprese: l'alterazione di dati e/o programmi, lo spionaggio informatico, l'utilizzazione non autorizzata di un programma informatico protetto.

[31] La legge 23.12.1993, n. 547, recante modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, ha introdotto le seguenti fattispecie delittuose: "*Accesso abusivo ad un sistema informatico o telematico*" (art. 615-*ter* c.p.), "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*" (art. 615-*quater* c.p.), "*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*" (art. 615-*quinquies* c.p.), "*Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche*" (art. 617-*bis* c.p.), "*Falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche*" (art. 617-*ter* c.p.), "*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*" (art. 617-*quater* c.p.), "*Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche*" (art. 617-*quinquies* c.p.), "*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche* (art. 617-*sexies* c.p.), "*Frode informatica*" (art. 640-*ter* c.p.).

[32] Per un esame della disciplina dei *computer crimes*, con particolare attenzione per la distinzione fra reati necessariamente ed eventualmente informatici, si rinvia a L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in

A seconda del ruolo rivestito dal *computer* nella struttura del fatto tipico, la dottrina ha individuato due sotto-categorie dei reati in parola.

I *computer crimes in senso stretto* (o *necessariamente informatici*) consistono in quei fatti che, per assumere penale rilevanza, postulano che la condotta, posta in essere attraverso il *device*, sia volta ad arrecare offesa all'integrità del sistema informatico collegato ad un diverso *device* preso di mira (quale oggetto materiale del reato)[33].

Diversamente, nel caso dei cosiddetti *reati eventualmente informatici* (o *computer facilitated crimes*), i *devices* rappresentano dei meri mezzi per realizzare, attraverso modalità informatiche, condotte che, di per sé, sono già penalmente rilevanti, sempre rivolte ad un *device* o al relativo sistema collegato (oggetto materiale)[34].

Quanto al bene giuridico offeso dai reati informatici, ad oggi il legislatore italiano non ha provveduto ad individuarne uno di autonomo, potendo rilevare interessi quali l'*inviolabilità del domicilio*[35], l'*inviolabilità dei segreti*[36] o il

---

Id. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, CEDAM, 2004, pp. 21 e ss.; L. LEVITA, *Reati informatici. Disciplina sostanziale e questioni processuali*, Giuffrè, 2012, pp. 3 e ss.

[33] L. LEVITA, I reati informatici. *Disciplina sostanziale e questioni processuali*, op. cit., pp. 3-44. Esempio di reato necessariamente informatico è l'"*Accesso abusivo ad un sistema informatico o telematico*" (art. 615-*ter* c.p.).

[34] L. LEVITA, *ibidem*, pp. 45-100. Esempio di reato eventualmente informatico è la "*Frode informatica*" (art. 640-*ter* c.p.).

[35] I delitti di "*Accesso abusivo ad un sistema informatico o telematico*" (art. 615-*ter* c.p.), "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*" (art. 615-*quater* c.p.), "*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*" (art. 615-*quinquies* c.p.) sono ricompresi nella Sezione IV del Titolo XII del Libro II del codice penale, dedicata ai delitti contro l'*inviolabilità del domicilio*.

[36] I delitti di "*Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche*" (art. 617-*bis* c.p.), "*Falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche*" (art. 617-*ter* c.p.), "*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*" (art. 617-*quater* c.p.), "*Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche*" (art. 617-*quinquies* c.p.) e "*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*" (art. 617-*sexies* c.p.) sono ricompresi nella Sezione V del Titolo XII, del Libro II del codice penale, dedicata ai delitti contro l'*inviolabilità dei segreti*.

patrimonio[37]. Tuttavia la più recente giurisprudenza di legittimità pronunciatasi in materia e autorevole parte della dottrina sono concordi nel ritenere che l'offesa informatica sia rivolta all'*integrità* e all'*inviolabilità dei sistemi informatici*[38]. Pertanto sarebbe opportuno aggiornare il codice penale, introducendo un nuovo Titolo che raggruppi tutti i delitti (informatici) che colpiscono tale peculiare interesse giuridico.

I *reati cibernetici*, invece, hanno avuto diffusione a partire dalla fine degli anni '90 dello scorso secolo, in coincidenza con l'avvio del processo che ha portato all'utilizzo massivo di Internet e, quindi, della fase cibernetica della rivoluzione tecnologica. Tale liberalizzazione ha consentito di valorizzare il ruolo del *cyberspace*, che è divenuto centrale nello svolgimento dei rapporti sociali fra i soggetti e, di riflesso, nella perpetrazione di nuovi delitti[39].

---

[37] Il delitto di "*Frode informatica*" (art. 640-*ter* c.p.) è ricompreso nel Capo II del Titolo XIII del Libro II del codice penale, dedicato ai delitti contro il patrimonio mediante frode.

[38] Per quanto riguarda la giurisprudenza *ex multis* Cass. pen., Sez. II, sent. 20.5.2019 (ud. 14.1.2019), n. 21987, in cui i giudici - nel definire con acribia i rapporti intercorrenti tra i delitti di "*Accesso abusivo a sistema informatico*", "*Frode informatica* e *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*" - hanno chiarito che, sebbene il delitto *ex* art. 640-*ter* c.p. possa involgere interessi patrimoniali, esso offende in via principale la *regolarità del funzionamento degli apparecchi informatici*, la *riservatezza dei dati*, nonché la *certezza del traffico giuridico-informatico*. Per un esame delle questioni più rilevanti affrontate nella pronuncia si rinvia a M. BORGOBELLO, *La Cassazione sul rapporto tra accesso abusivo a sistema informatico, frode informatica e detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*, in *Giur. Pen.,* 20.1.2020. Per quanto riguarda la dottrina, invece, C. LARINNI, *Garantismo europeista: un ossimoro?*, *op. cit.*, p. 11 e ss.; F. BERGHELLA, R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 9/1995, pp. 2329 e ss.; L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, op. cit., pp. 21 e ss.

[39] Cfr. P. M. SABELLA, *Il fenomeno del cybercrime nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali,* in *Informatica e diritto,* Vol. XXVI, 1/2017, pp. 148 e ss. in cui si legge che: «Il cybercrime può essere definito come un comportamento delittuoso posto in essere mediante l'uso distorto o abusivo dei sistemi hardware e software, comprendenti genericamente l'accesso illegale, la manipolazione e l'intercettazione di dati, l'interferenza con il corretto funzionamento di strumenti informatici e l'uso improprio di dispositivi, contraddistinto tendenzialmente dalla coesistenza di alcuni elementi quali: a) l'anonimato del soggetto attivo o la sua difficoltosa reperibilità; b) l'automatizzazione parziale o totale della condotta; c) la significativa intensità del momento volitivo del dolo; d)

Il legislatore europeo ha dimostrato grande attenzione per le interazioni fra tecnologia cibernetica e diritto penale, predisponendo tempestivamente la Convenzione di Budapest sul *cybercrime* del 2001, la quale, attualmente, resta l'unico atto espressamente dedicato alla materia[40].

La *ratio*, che ha animato il legislatore sovranazionale nella predisposizione della Convenzione, consiste nel promuovere l'adozione, da parte degli Stati membri, di sistemi di tutela appositamente dedicati ai nuovi reati commessi nel *cyberspace*. Tale obbiettivo emerge dall'esame della struttura della stessa Convenzione ed in particolare della Sezione I (intitolata "*Diritto penale materiale*") del Capitolo II (intitolato "*Provvedimenti da adottare a livello nazionale*"), la quale - nei suoi cinque Titoli - raccoglie la descrizione dettagliata delle condotte di un gran numero di reati, che ogni Stato membro è chiamato a tipizzare e punire adeguatamente[41]. Coerentemente, la relativa Sezione II (intitolata "*Diritto procedurale*") predispone un complesso sistema di misure processuali, attraverso le quali il legislatore si preoccupa di offrire garanzie in ordine alla conservazione dei dati e delle informazioni personali[42].

Il nostro Paese ha ratificato la Convenzione di Budapest solo nel 2008, con la legge 18.3.2008, n. 48, scegliendo di non introdurre nel nostro ordinamento il

---

l'indebolimento delle coordinate spazio-temporali per una corretta identificazione del tempus e del *locus commissi delicti*».

[40] Sul punto rileva osservare che la *criminalità informatica* è una delle «sfere di criminalità» rispetto alle quali il Parlamento europeo ed il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni (art. 83 TFUE).

[41] La struttura della Convenzione può schematicamente essere suddivisa in tre parti. La prima attiene alla definizione delle condotte criminali che devono essere incluse nei codici penali dei diversi Paesi. La seconda, invece, riguarda questioni di ordine processuale. La terza parte, infine, attiene alle procedure di cooperazione internazionale da adottare al fine di creare una disciplina uniforme a livello europeo, che si riverberi sia in punto di fattispecie sia in punto di investigazioni.

[42] Così, ad esempio, ciascuno Stato deve assicurare alle Autorità competenti i poteri necessari per ordinare ad un fornitore di servizi, che offre le proprie prestazioni sul territorio nazionale, di fornire i dati in suo possesso (o comunque sotto il suo controllo) relativi agli utenti (art. 18, co. 1).

concetto di «reato cibernetico» e, in ogni caso, senza adottare strumenti realmente efficaci contro la minaccia *cyber*[43].

Invero, dopo quindici anni dall'attuazione della Convenzione durante i quali lo sviluppo tecnologico è progredito inesorabilmente, nel codice penale italiano non si rinvengono ancora riferimenti al concetto di *cibernetica*, continuandosi ad usare esclusivamente quello di *informatica*. Nonostante la scelta del legislatore domestico, la quale rivela come non si sia ancora compresa la portata del fenomeno dei *cybercrimes*, è in ogni caso indispensabile fornire una definizione degli stessi.

I *reati cibernetici* (diversamente dai *computer crimes*) sono i reati commessi nel *cyberspazio*, che è l'elemento essenziale che ne caratterizza il fatto tipico. Essi sono pertanto interessati dalle stesse criticità che affliggono lo spazio virtuale, quale non-luogo deterritorializzato, detemporalizzato e depersonalizzato[44].

In proposito si pensi alla possibilità di creare, da parte degli utenti della rete (e specificamente dei *social networks*), i cosiddetti *fake profiles,* che consentono di celare la propria identità, con conseguenti difficoltà in ordine all'individuazione del soggetto agente e all'accertamento della colpevolezza[45].

Sotto il profilo oggettivo, la *condotta* dei reati cibernetici consiste in comportamenti che rilevano in relazione a reati già previsti dal codice penale. Sul punto, solo a titolo esemplificativo, si pensi al *cyberbullismo*, il quale, ancorché rimanga privo di una tipizzazione nel codice penale, può consistere (sotto il

---

[43] Per un esame della legge di ratifica 18.3.2008, n. 48 si veda L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* , in *Dir. Pen. e Proc.*, 6/2008, pp. 696 e ss.

[44] Sul punto L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, *op. cit.*, p. 827 e ss., in cui l'autore propone una *summa divisio*, distinguendo i reati cibernetici «in senso stretto» (ovverosia i reati che, già a livello di tipizzazione legislativa, richiedono necessariamente fra gli elementi costitutivi il *cyberspace* e delle condotte cibernetiche nel senso predetto, v. §. 4, nonché §. 2.2. di questo Capitolo) dai reati informatici «in senso ampio» (ovverosia i reati che si caratterizzano per trovare nel *cyberspace* solo una peculiare modalità di realizzazione e di aggressione).

[45] Per un esame delle questioni giuridiche che emergono in relazione ai *social networks* si rinvia a F. COLAPAOLI, A. COPPOLA, M. R. GRAZIANI, M. MIRONI, *I social network*, in AA.VV., *Social network e diritto*, Giappichelli, 2021, pp. 1 e ss.

profilo oggettivo) in: «*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line* […]» (art. 1, co. 2, l. 29.5.2017, n. 71)[46].

Ad ogni buon conto la condotta dei *cybercrimes* si caratterizza per la *natura* cibernetica e per le particolarità del *contesto* in cui essa è posta in essere[47]. Invero, come si è detto, i *cybercrimes* sono commessi nel cyberspazio e presentano una maggior pervasività (innanzitutto rispetto ai reati informatici) proprio in ragione delle peculiarità che lo interessano. Invero il soggetto agente, grazie alle nuove tecnologie, è in grado di reperire informazioni sensibili anche senza che l'interessato le condivida pubblicamente[48]. Inoltre le condotte cibernetiche sono connotate dalla capacità di elaborare le informazioni e i dati raccolti mediante l'impiego di complessi algoritmi[49].

Per quanto riguarda il ruolo dei *computers* e dei sistemi informatici nell'integrazione dei *cybercrimes,* essi possono tutt'al più rappresentare degli strumenti attraverso i quali porre in essere le condotte cibernetiche, senza i quali il fatto non perde rilevanza penale. Più nello specifico, il *computer* resta uno dei mezzi di cui il soggetto agente può servirsi per "traferirsi" dalla dimensione reale a quella virtuale (ove porre in essere i comportamenti rilevanti) e non, invece,

---

[46] Per un inquadramento giuridico del fenomeno del cyberbullismo si rinvia a V. SELLAROLI, *Il nuovo reato di cyberbullismo (l. 29 maggio 2017, n. 71)*, Giuffrè, 2017, pp. 10 e ss.

[47] Per un esame della tipizzazione normativa che dovrebbe ricevere il fatto di reato cibernetico si veda I. SALVADORI, *Il diritto penale dei software a duplice uso,* in AA.VV., R. WENIN, G. FORNASARI (a cura di)*, Diritto penale e modernità. Le nuove sfide fra terrorismo*, *sviluppo tecnologico e garanzie fondamentali*, op. cit., p. 361 e ss.

[48] Si pensi in proposito alle condotte di *phishing* e di *pharming*.

[49] P. M. SABELLA, *Il fenomeno dei cybercrimes nello spazio giuridico contemporaneo*, op. cit., pp. 148 e ss.

l'oggetto materiale del reato né il bene giuridico da tutelare nella sua integrità (come invece accade nei *computer crimes*)[50].

Per quanto attiene al profilo psicologico, i reati cibernetici si connotano per il dolo specifico, con finalità di volta in volta individuate dal legislatore. Sul punto si pensi al caso del *cyberbullismo*, rispetto al quale, per espressa previsione della definizione contenuta nell'art. 1, co. 2., l. 71/2017, la finalità perseguita dal soggetto agente consiste nell'isolare un minore o un gruppo di minori, ponendo in atto un serio abuso, un attacco dannoso o la loro messa in ridicolo[51].

Il reato cibernetico commesso con finalità di terrorismo, invece, è il *cyberterrorismo*, il quale - come emergerà dalla ricerca condotta nel prosieguo di questo lavoro - si connota per un ulteriore specifico scopo rispetto a quelli già tipizzati dall'art. 270-*sexies* c.p.[52].

Invero i *cybercrimes* determinati da motivi politici (art. 8 c.p.) hanno suscitato l'interesse della dottrina, che ha qualificato come tali (oltre al cyberterrorismo) anche il *cyberhactivism* e il *cyberspionage*.

Il primo è il *cybercrime* che consiste nel porre in essere attacchi *hacker* che danneggiano le strutture informatiche dello Stato. Trattasi di un reato proprio, dal momento che le condotte rilevanti vengono realizzate dai cosiddetti *hackers.* Questi sono dotati di approfondite conoscenze informatiche – in genere acquisite all'esito di percorsi di studi superiori – e animati da peculiari finalità ideologiche,

---

[50] L. PICOTTI, *Quale diritto penale nella dimensione globale del cyberspace*?, in AA.VV., R. WENIN, G. FORNASARI (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, op. cit., pp. 310 e ss.

[51] V. SELLAROLI, *Il nuovo reato di cyberbullismo (l. 29 maggio 2017, n. 71)*, op. cit., pp. 10 e ss.

[52] Sul concetto di cyberterrorismo si veda D. COHEN, *L'evoluzione del terrorismo contemporaneo nel cyber-spazio*, in *Gnosis*, 2/2016, p. 118 ss.; R. PINO, *Il "cyberterrorismo": un'introduzione,* in *Ciberspazio e diritto: rivista di informatica giuridica*, 3/2013, p. 430; A. F. VIGNERI, *Cyberterrorismo: realtà o finzione?,* op. cit., pp. 8 e ss.; R. FLOR, *Cyberterrorismo e diritto penale in Italia*, in AA.VV., R. WENIN, G. FORNASARI (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, op. cit., pp. 325 e ss.

che possono perseguire individualmente o anche organizzati in complesse strutture[53].

Il *cyberespionage*, invece, presuppone condotte finalizzate a sfruttare le potenzialità e le dinamiche di Internet per sottrarre informazioni segrete che riguardino lo Stato. Tra i settori notoriamente più colpiti da questa forma di *cybercrime* merita menzione quello militare. In questo caso il *cyberspionage* è commesso al fine di conoscere progetti e documenti appartenenti a forze armate straniere e raggiungere una superiorità strategica in ambito bellico[54].

Profili di criticità emergono anche in relazione all'individuazione del *locus* e del *tempus commissi delicti* dei *cybercrimes*.

Sul punto, la dottrinata ha evidenziato che l'evento cibernetico si connota per un'ulteriore fase di "prolungamento", successiva a quella del perfezionamento[55]. Tale peculiarità impone, dunque, di indagare i presupposti ed i limiti in relazione ai quali può dirsi esercitato e mantenuto, ai fini della responsabilità penale, il controllo umano sul decorso dell'*iter criminis*, anche in relazione agli effetti che possono prodursi a grande distanza di tempo e a prescindere da ulteriori comportamenti umani. Secondo la dottrina, il fenomeno in questione, che è peculiare dei *cybercrimes*, non pare riconducibile al paradigma del *reato permanente*. Infatti questo, come noto, presuppone la costante dipendenza della protrazione dell'offesa al bene giuridico dalla contemporanea

---

[53] S. LAY, M. PASCARELLA, *Hacktivismo, cyberterrorismo e misure di contrasto*, The Alpha Institute of Geopolitics and Intelligence, 2016, pp. 5 e ss.

[54] A. SPAGNOLO, S. SALUZZO, *La responsabilità degli Stati e delle organizzazioni internazionali nuove fattispecie, problemi di attribuzione e di accertamento*, Ledizioni, 2017, pp. 22 e ss.

[55] L. PICOTTI, *Reati informatici, riservatezza, identità digitale*, in AIDP, 2004, p. 16, in cui l'autore spiega che «il reato cibernetico non può dirsi di norma "esaurito" nel periodo intermedio, anche assai lungo, che può intercorrere fra i due momenti, in cui "permane" e si approfondisce l'offesa». Si pensi, solo a titolo esemplificativo, alle conseguenze del *cyberbullismo*, della diffamazione *on line*, della diffusione di pedopornografia, dell'istigazione e propaganda di atti di odio e discriminazione razziale, della distribuzione o messa a disposizione di opere digitali in violazione dei diritti d'autore, delle molteplici violazioni della riservatezza e della *privacy*.

condotta volontaria del reo, il quale potrebbe in ogni momento farla cessare[56]. La peculiare forma di manifestazione dei reati cibernetici non sembra potersi ricondurre neppure entro lo schema del *reato a consumazione prolungata*. In questo caso, infatti, la fase della consumazione, che si presenta frazionata, presuppone il compimento di più atti realizzativi, tra i quali può anche intercorrere un significativo lasso di tempo[57].

Per quanto attiene al *locus commissi delicti*, invece, la dematerializzazione che connota il cyberspazio, ove vengono poste in essere le condotte dei reati cibernetici, non consente di applicare *tout court* le categorie tradizionalmente previste per la sua determinazione. Della questione ci si occuperà diffusamente nel paragrafo successivo (v. *infra* §. 4.1.)[58].

In conclusione, si ritiene che i reati cibernetici – che si differenziano dai *computer crimes* - non possano essere qualificati alla stregua di mere modalità alternative (speciali) per la realizzazione di reati comuni già previsti e puniti dal codice penale. Invero le caratteristiche dei *cybercrimes*, sia sotto il profilo oggettivo che soggettivo, impongono al legislatore di introdurre una nuova categoria di reati, la quale, dogmaticamente, tenga conto delle criticità della cibernetica (e del cyberspazio), tipizzando adeguatamente il fenomeno criminoso

---

[56] L. PICOTTI*, ibidem*, p. 16.

[57] Per un approfondimento sul concetto di reato a consumazione prolungata si rinvia a F. MANTOVANI, *Diritto penale. Parte speciale*, CEDAM, 2019, pp. 191 e ss.; C. BENUSSI, D. BRUNELLI, *Il reato portato a conseguenze ulteriori, problemi di qualificazione giuridica*, Giappichelli, 2000, pp. 105 e ss. Sul punto giova osservare che la giurisprudenza ha impiegato il concetto di reato a consumazione prolungata per descrivere perlopiù i delitti in cui la fase consumativa postula la dazione, da parte della persona offesa, di una somma di denaro a favore del soggetto agente, la cui erogazione avviene a rate o in *tranches*. Con riguardo alla configurabilità del reato di "*truffa a rate*" Cass. pen., Sez. II, sent. 9.1.2018, n. 295; Cass. pen., Sez. II, sent. 2.12.2016, n. 53667; Cass. pen., Sez. V, sent. 11.6.2014, n. 32050. In riferimento alla qualificazione del delitto di indebita percezione di erogazioni ai danni dello Stato come reato a consumazione prolungata, invece, Cass. pen., Sez. II, 9.3.2015, n. 26761; Cass. pen., Sez. III, 8.10.2014, n. 6809; Cass. pen., Sez. VI, 19.2.2013, n. 12625.

[58] Per un esame dei problemi che attengono all'individuazione del *locus commissi delicti* dei *cybercrimes* - che verrà approfondito nel prosieguo - si rinvia a I. SALVADORI, *Il diritto penale dei software a duplice uso,* op. cit., p. 324; R. RAZZANTE, A. CRISTALLINI, *Cybercrime tra diritto ed economia*, Pacini, 2021, pp. 31 e ss.; R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in AA.VV., A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrimes*, UTET, 2019, pp. 150 e ss.

in parola. A tal fine sarà indispensabile interrogarsi sull'esistenza di un autonomo bene giuridico di categoria al quale si rivolge l'offesa dei reati cibernetici e, eventualmente, individuarne il fondamento costituzionale (v. *infra* §. 4.2. e 4.3.).

4.1. Quale locus commissi delicti nel cyberspazio? La risposta della giurisprudenza

Prima di procedere nella trattazione e dedicarsi alla ricerca del bene giuridico comune ai *cybercrimes*, si ritiene opportuno completare il quadro giuridico illustrato nel precedente paragrafo, approfondendo le cennate questioni attinenti all'individuazione del *locus commissi delicti* dei *cybercrimes*, alla luce delle pronunce di legittimità sul tema. Invero la complessità del *cyberspace*, come non-luogo deterritorializzato non perimetrabile, impongono di adeguare le categorie del diritto penale tradizionalmente impiegate in materia.

Sul punto è preliminarmente opportuno ricordare che, nel nostro ordinamento, la disciplina del luogo della commissione del reato trova fondamento nell'art. 6 del codice penale. La disposizione prevede che il reato si considera commesso nel territorio dello Stato se ivi si è svolta la condotta (tutta o in parte) o si è verificato l'evento.

Trattasi del *principio di territorialità*, che, tuttavia, presenta evidenti difficoltà applicative con riguardo ai reati cibernetici, i quali, come si è detto, si svolgono in una dimensione dematerializzata e deterritorializzata[59].

---

[59] S. SEMINARA, *Locus commissi delicti*, *Giurisdizione e competenza nel cyberspazio*, intervento al Convegno intitolato "*Presi nella rete: analisi e contrasto alla criminalità informatica*", 2012, p. 1, disponibile nel sito dell'Università degli Studi di Pavia *link*: *www.informaticagiuridica.unipv.it,* in cui si legge che: «Internet ignora i confini territoriali e, dunque, la territorialità degli ordinamenti giuridici; […] gli ordinamenti giuridici necessitano invece di uno spazio sul quale esercitare la propria sovranità esclusiva e ulteriormente tendono ad allargare i propri confini applicativi sulla base di valutazioni legate alla qualità del soggetto attivo o del soggetto passivo o alla natura del reato commesso. È ovvio che queste due constatazioni operano in senso antitetico, determinando lo scontro fra un mondo virtuale ed uno reale».

Neppure le fonti europee risolvono le criticità connesse al *locus commissi delicti* dei reati cibernetici.

L'art. 22 della Convenzione di Budapest adotta il *criterio della territorialità*, salvo precisare che, laddove il reato cibernetico sia punibile nel luogo in cui è stato commesso ovvero non rientri nella competenza territoriale di nessuno Stato, deve impiegarsi il *principio della personalità attiva*, che individua la legge applicabile in base alla nazionalità del soggetto attivo.

L'art. 10 della decisione-quadro 2005/222/GAI, relativa agli attacchi contro i sistemi di informazione (adottata il 24 febbraio 2005), invece, prospetta alternativamente i criteri della *territorialità*, della *personalità attiva* e - relativamente alle sole persone giuridiche - del *destinatario del profitto*.

In un così variegato ed incerto panorama di criteri e nella perdurante mancanza di uno specifico intervento del legislatore nazionale, la giurisprudenza domestica (sia di merito che di legittimità) ha cercato di risolvere le criticità che riguardano il *locus commissi delicti* dei reati commessi nel *cyberspace* in via ermeneutica, adottano orientamenti diversi nel corso del tempo.

Prima di procedere all'esame delle decisioni più rilevanti in materia, è necessario sgombrare il campo da equivoci con un chiarimento. Le sentenze a cui si farà riferimento, pur occupandosi direttamente dei reati informatici e in particolare dell'"*Accesso abusivo ad un sistema informatico o telematico*" (art. 615-*ter* c.p.) - attese le lacune in materia di reati cibernetici -, hanno affrontato la questione in termini più generali, indagando i criteri per l'individuazione del *locus commissi delicti* nel cyberspazio. Conseguentemente, le conclusioni a cui sono pervenuti i giudici rilevano anche rispetto ai *cybercrimes*, che, per definizione, sono i reati commessi nello spazio cibernetico.

Inizialmente la Cassazione era orientata nel ritenere che il *locus commissi delicti* dei reati in parola corrispondesse a quello ove è fisicamente collocato l'oggetto materiale della condotta criminosa, ovverosia il *server* o il sistema

informatico rispetto ai quali viene posta in essere la violazione o l'accesso abusivo[60].

Sebbene l'orientamento in parola sia pienamente rispettoso dei criteri tradizionali di fisicità e materialità - che, come noto, fanno riferimento al luogo della consumazione del reato - esso, allo stesso tempo, ignora le peculiarità che connotano la circolazione dei dati in rete. Tra queste figura la consultabilità dei dati contemporaneamente da parte di più utenti, anche qualora si trovino a migliaia di chilometri di distanza tra loro[61].

Parte della dottrina ha evidenziato che questo primo orientamento, sebbene coerente con i tradizionali criteri spaziali adottati in diritto penale, ignora le peculiarità del *cyberspace*. Inoltre si è osservato che, facendo coincidere il *locus commissi delicti* con la collocazione dell'oggetto materiale del reato, nel caso di molteplici accessi abusivi al medesimo sistema informatico, ciascuno dei procedimenti ad essi relativi sarebbero soggetti alla competenza territoriale dello stesso giudice, con conseguenze negative in relazione al buon andamento dell'attività di accertamento della responsabilità penale[62].

La giurisprudenza successiva dimostrava maggiore attenzione ai rapporti intercorrenti fra *cyberspace*, tecnologia e diritto penale.

Con Ordinanza 16.4.2014, il Giudice per l'Udienza Preliminare del Tribunale di Roma - sollevando un conflitto di competenza fra il Tribunale capitolino e quello di Firenze (*ex* art. 28 c.p.p.) - evidenziava che, con riguardo al

---

[60] *Ex multis* Cass. pen., Sez. I, sent. 27.5.2013, n. 40303. Per un commento della pronuncia si rinvia a C. PECORELLA, *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo a un sistema informatico o telematico e commento*, in *Dir. Pen. Comp.*, 11.10.2013 (*https://archiviodpc.dirittopenaleuomo.org/d/2536–la–cassazione–sulla–competenza–territoriale–per–il-delitto–di–accesso–abusivo–a–un-sistemainformat#:~:text=la%20I%20Sez.-, pen.,tra%20quelli%20contestati%20agli%20imputati*).

[61] R. FLOR, *Art. 615-ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. Pen. Proc.*, 1.1.2008, p. 134 e ss. Le pronunce conformi a questo primo orientamento adottano un'interpretazione sistematica, focalizzando l'attenzione sulla collocazione codicistica dell'art. 615-*ter* c.p. e ritenendo – concordemente al legislatore - che il bene giuridico offeso dai *computer crimes* sia la mera inviolabilità del domicilio informatico.

[62] C. PECORELLA, *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo a un sistema informatico o telematico*, op. cit.

locus commissi delicti dei reati commessi nel *cyberspace*, non è possibile procedere ad una delimitazione di uno luogo fisicamente circoscritto rispetto al quale esercitare lo *ius excludendi alios* secondo i criteri tradizionali[63]. Per il GUP tale impossibilità è legata alla natura stessa del *cyberspace*, che è una dimensione delocalizzata e deve intendersi come una rete di comunicazione in cui «tutto è contestualmente presente in tutti gli ambiti in cui il sistema opera»[64]. Infatti, come si è precedentemente osservato, gli utenti del cyberspazio possono potenzialmente accedere al medesimo gruppo di informazioni nello stesso momento e da qualsiasi luogo in cui essi si trovino. Ebbene, secondo il GUP romano, solo la condotta umana di ingresso abusivo è assoggettata ai criteri spaziali del mondo fisico tradizionalmente impiegati in diritto penale e si esaurisce nel luogo in cui viene digitato il tasto d'accesso al sistema informatico[65].

Con la sentenza del 15.7.2014, n. 34165, la Cassazione, chiamata a risolvere il conflitto di competenza prefato, si pronunciava in favore del Tribunale

---

[63] GUP presso il Tribunale Roma, ordinanza del 16.4.2014. Oggetto del relativo procedimento erano le condotte di alcuni pubblici ufficiali che dal loro ufficio di Firenze avevano compiuto un accesso abusivo alla banca dati riservata del Sistema d'Informazione Interforze del Ministero dell'Interno (SDI) sito in Roma.

[64] C.F. GROSSO, *Su di un'interessante controversia interpretativa in tema di luogo del commesso reato e di giudice competente per territorio in materia di accesso abusivo in un sistema informatico*, in *Riv. it. dir. proc. pen.*, 2014, pp. 1704 e ss. Il riferimento allo *ius excludendi alios* rimanda inequivocabilmente al tratto caratterizzante del domicilio, di cui il legislatore penale intende tutelare l'inviolabilità. Sostenere l'incompatibilità del diritto-potere di escludere con il *cyberspace* significa dunque rifiutare di ricondurre quest'ultimo entro gli schemi del domicilio.

[65] GUP presso il Tribunale di Roma, cit., in cui si legge: «Il delitto di accesso abusivo in un sistema informatico o telematico si consuma nel luogo in cui viene digitato il tasto d'ingresso nel sistema informatico e, pertanto, nella sede periferica del sistema presso la quale tale condotta è compiuta. L'introduzione avviene infatti nelle singole sedi periferiche e s'inserisce contestualmente nel sistema informatico centrale; tutto è contestualmente presente in tutti gli ambiti in cui il sistema opera (la banca dati centrale: come le sedi periferiche), non esistendo una ripartizione spaziale poiché si versa in un *cyberspazio delocalizzato*, in una rete di comunicazione telematica. L'unica cosa collocabile – secondo i parametri del mondo fisico, ben diverso da quello informatico – è la condotta umana, che finisce nelle sedi locali, con contegni non più arginabili negli esiti, e contestualmente produce modifiche nel sistema centrale. E' del tutto erroneo scindere il *server* […] poiché il sistema è un *unicum* che si alimenta di continue allegazioni e acquisizioni di dati contestualmente ovunque presenti. Luogo del commesso reato e giudice competente per territorio sono pertanto il luogo in cui viene digitato il tasto di accesso al sistema informatico ed il giudice competente su quel luogo».

di Roma, riconoscendone la competenza per connessione in riferimento ad altri fatti (art. 12 c.p.p.). I giudici di legittimità condividevano le argomentazioni del GUP e, discostandosi dal primo orientamento giurisprudenziale, affermavano che: «in astratto le osservazioni del Pubblico Ministero, che ha sollecitato il conflitto e del giudice che l'ha sollevato, così come quelle delle parti intervenute, hanno il pregio di sviscerare con maestria argomenti scientifici e giuridici, dibattuti sia in giurisprudenza sia in dottrina, meritevoli di attento vaglio critico, attesa la rilevanza delle questioni agitate e la ricordata incidenza su procedimenti che risultano svolti in ambiti territoriali diversi»[66].

Successivamente, la prima Sezione penale dalla Corte di Cassazione, rilevati - in un diverso processo - i contrastanti orientamenti giurisprudenziali e dottrinali registratisi in materia, rimetteva - con ordinanza del 28.10.2014, n. 52575 - la questione relativa all'individuazione del *locus commissi delicti* nel *cyberspace* (in particolare in riferimento al delitto *ex* art. 615-*ter* c.p.)[67] alle Sezioni Unite, che si sono pronunciate con la sentenza del 24.4.2015, n. 17325[68].

---

[66] Cass. pen., Sez. I, sent. 15.7.2014, n. 34165. Per un esame della pronuncia si rinvia a M. BELLACOSA, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle sezioni unite*, in *Dir. Pen. Comp.*, 2.2.2015, p. 2, che nell'argomentazione della Cassazione intravede un'avvisaglia verso un mutamento di orientamento relativo all'individuazione del luogo del commesso delitto in materia di reati informatici.

[67] Cass. pen., Sez. I, ord. 28.10.2014, n. 52575, in cui si legge: «Poiché il reato si perfeziona con l'introduzione abusiva nel sistema, a prescindere dalla effettiva acquisizione dei dati riservati in esso contenuti, si deve ritenere che la condotta materiale si perfeziona nel luogo fisico e nel momento in cui l'agente si introduce abusivamente nella postazione locale (nel caso in esame nel computer ubicato presso la sede della Motorizzazione Civile di Napoli), la quale non è un mero mezzo di accesso ma, al pari del computer denominato server ubicato presso la sede centrale, un componente informatico essenziale costituente articolazione territoriale del complessivo sistema informatico nazionale nella disponibilità del Ministero dei Trasporti». Il caso *de quo* riguardava l'accesso abusivo e ripetuto nel sistema informatico del Ministero delle Infrastrutture e dei Trasporti da parte di un'impiegata della motorizzazione civile (in concorso con altri soggetti), al fine di effettuare visure elettroniche che esulavano dalle sue mansioni ed interessavano l'amministratore di un'agenzia di pratiche automobilistiche.

[68] Cass., pen., SS.UU., sent. 24.4.2015, n. 17325, di cui si riporta la massima, tratta da P. CIPOLLA, sub *Art. 615-ter c.p.*, in AA.VV., G. LATTANZI (a cura di), *Codice penale annotato con la giurisprudenza*, Giuffrè, 2020, p. 1993: «In tema di acceso abusivo ad un sistema informatico o telematico, il luogo di consumazione del delitto di cui all'art. 615-*ter* c.p. coincide con quello in cui si trova l'utente che, tramite elaboratore elettronico o altro dispositivo per il

Il Supremo Consesso, preliminarmente, evidenzia come la *ratio* che ha animato il legislatore nella previsione della fattispecie *ex* art. 615-*ter* c.p. fosse assicurare la protezione del domicilio informatico, il quale, contenendo dati ed informazioni sensibili dell'utente, merita di essere tutelato come emblematico diritto della sfera individuale.

Tuttavia i giudici negano qualsivoglia corrispondenza fra il domicilio informatico e quello reale, affermando che i criteri tradizionalmente impiegati per collocare la condotta nel tempo e nello spazio entrano in crisi se applicati al *cyberspace*, dal momento che questo consiste in una dimensione dematerializzata, connotata dalla delocalizzazione delle risorse e dei contenuti[69].

In secondo luogo le Sezioni Unite osservano che la fattispecie di cui all'art. 615-*ter* c.p., che è di mera condotta, non è volta a proteggere esclusivamente il cosiddetto domicilio informatico, ma offre una tutela anticipata ad una pluralità di beni giuridici e di interessi eterogenei tra loro. Questi non

---

trattamento automatico dei dati, digitando la "parola chiave" o altrimenti eseguendo la procedura di autenticazione, supera le misure di sicurezza apposte dal titolare per selezionare gli accessi e per tutelare la banca-dati memorizzata all'interno del sistema centrale ovvero vi si mantiene eccedendo i limiti dell'autorizzazione ricevuta». In motivazione la Corte ha specificato che il sistema telematico per il trattamento dei dati condivisi tra più postazioni è unitario e, per la sua capacità di rendere disponibili le informazioni in condizioni di parità a tutti gli utenti abilitati, assume rilevanza il luogo di ubicazione della postazione remota dalla quale avviene l'accesso e non invece il luogo in cui si trova l'elaboratore centrale.

[69] Cass. pen., SS.UU., sent. 24.4.2015, n. 17325, p. 7, in cui emerge che i criteri tradizionali non sono applicabili al *cyberspace*, siccome elaborati per «una realtà fisica, nella quale le conseguenze sono percepibili e verificabili con immediatezza». Inoltre, nella pagina successiva della sentenza in esame (p. 8), si legge: «È stato notato che nel *cyberspace* i criteri tradizionali per collocare le condotte umane nel tempo e nello spazio entrano in crisi, in quanto viene in considerazione una dimensione "smaterializzata" (dei dati e delle informazioni raccolti e scambiati in un contesto virtuale senza contatto diretto o intervento fisico su di essi) ed una complessiva "delocalizzazione" delle risorse e dei contenuti (situabili in una sorte di meta-territorio). Pertanto non è sempre agevole individuare con certezza una sfera spaziale suscettibile di tutela in un sistema telematico, che opera e si connette ad altri terminali mediante reti e protocolli di comunicazione. Del resto, la dimensione aterittoriale si è incrementata da ultimo con la diffusione dei dispositivi mobili (*tablet*, *smartphone*, sistemi portatili) e del *cloud computing*, che permettono di memorizzare, elaborare e condividere informazioni su piattaforme delocalizzate dalle quali è possibile accedere da qualunque parte del globo».

interessano soltanto i contenuti personalissimi dei dati raccolti, ma si rivolgono anche a quelli di tipo economico-patrimoniale[70].

In un altro passaggio della sentenza, i giudici definiscono il concetto di *sistema informatico* come: «complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione (anche parziale) di tecnologie informatiche che sono caratterizzate, per mezzo di un'attività di "codificazione" e "decodificazione", dalla "registrazione" o "memorizzazione" tramite impulsi elettronici, su supporti adeguati, di "dati", cioè, di rappresentazioni elementari di un fatto, effettuata attraverso simboli (*bits*) in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare un insieme più o meno vasto di informazioni, organizzate secondo una logica che consente loro di esprimere un particolare significato per l'utente»[71]. Le Sezioni Unite mutuano la definizione dalla sentenza della Sesta Sezione penale del 4.10.1999, n. 3067, con alcune osservazioni[72]. Infatti i giudici, consapevoli dello sviluppo tecnologico registratosi in poco più di cinque lustri, precisano che, oggi, per sistema informatico si intende qualsiasi dispositivo che si caratterizzi per

---

[70] Cass. pen., SS.UU., sent. 24.4.2015, n. 17325, p. 6: «È condivisa l'opinione secondo la quale il delitto previsto dall'art. 615-*ter* c.p. è di mera condotta (ad eccezione per le ipotesi aggravate del comma secondo, nn. 2 e 3) e si perfeziona con la violazione del domicilio informatico - e, quindi, con la introduzione nel relativo sistema - senza la necessità che si verifichi una effettiva lesione del diritto alla riservatezza dei dati». Inoltre, i giudici aggiungo che: «La condotta è già abusiva (secondo la clausola di antigiuridicità speciale) nel momento in cui l'operatore non autorizzato accede al computer remoto e si fa riconoscere o autenticare manifestando, in tale modo, la sua volontà di introdursi illecitamente nel sistema con possibile violazione della integrità dei dati. Deve precisarsi in ogni caso che, se il server non risponde o non valida le credenziali, il reato si fermerà alla soglia del tentativo punibile» (p. 11). In senso conforme Cass. pen., Sez. V, sent. 6.2.2007, n. 11689.

[71] Sul punto giova osservare che la legge 23.12.1993, n. 547, recante modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, omette di fornire la definizione di *sistema informatico*, dandola per presupposta. Ad ogni buon conto, altra definizione fornita dalle Sezioni Unite nella pronuncia in esame è quella di «*accesso ad un sistema informatico*». Questo, secondo i giudici, «non coincide con l'ingresso all'interno del *server* fisicamente collocato in un determinato luogo», bensì con «l'introduzione telematica o virtuale, che avviene instaurando un colloquio elettronico o circuitale con il sistema centrale e con tutti i terminali ad esso collegati». Tale considerazione conferma la difficoltà di ricondurre entro gli schemi del domicilio tradizionale il bene giuridico tutelato.

[72] Cass. pen., Sez. VI, sent. 4.10.1999, n. 3067.

l'installazione di un *software* (che ne sovrintende il funzionamento), per la capacità di utilizzare periferiche o dispositivi esterni, per l'interconnessione con altri apparecchi e per la molteplicità dei dati trattati[73].

La scelta dei giudici di aggiornare la preesistente definizione attraverso i suddetti criteri risponde all'esigenza di elaborare un concetto quanto più ampio possibile di sistema informatico, onde evitare i vuoti di tutela che potrebbero originarsi per la difficoltà di inquadrare le più recenti novità tecnologiche entro i confini di una definizione troppo rigida.

Ad ogni modo, nel passaggio più rilevante della sentenza, si sostiene la necessità di aggiornare, con riferimento ai reati commessi nel *cyberspace*, le categorie tradizionalmente impiegate per l'individuazione del *locus commissi delicti*[74].

Infatti nella sentenza si legge che, nella realtà virtuale, il «concetto stesso di azione penalmente rilevante» subisce un'accentuata modificazione, fino a sfumare in impulsi elettronici[75]. Sul punto gli Ermellini aggiungono che «l'*input* rivolto al computer - da un atto umano consapevole e volontario - si traduce in un trasferimento - sotto forma di energie o *bit* - della volontà dall'operatore all'elaboratore elettronico, il quale procede poi automaticamente alle operazioni di codificazione, decodificazione, trattamento, trasmissione o memorizzazione di informazioni»[76].

Orbene, per tutte queste ragioni, ritenere che il luogo del commesso delitto coincida con quello ove è situato il *server* violato, si dimostra una soluzione che - pur pienamente rispettosa dei tradizionali schemi concettuali - non tiene conto che

---

[73] Cass. pen., SS.UU., sent. 24.4.2015, n. 17325, p. 7.

[74] Cass. pen., SS.UU., sent. 24.4.2015, n. 17325, p. 7: «La condotta illecita commessa in un ambiente informatico o telematico assume delle specifiche peculiarità per cui la tradizionale nozione - elaborata per una realtà fisica nella quale le conseguenze sono percepibili e verificabili con immediatezza - deve essere rivisitata e adeguata alla dimensione virtuale».

[75] Cass. pen., SS.UU., sent. 24.4.2015, n. 17325, pp. 7 - 8: «In altre parole, il concetto di azione penalmente rilevante subisce nella realtà virtuale una accentuata modificazione fino a sfumare in impulsi elettronici».

[76] Cass. pen., SS.UU., sent. 24.4.2015, n. 17325, p. 7. Tale passaggio sembra ricordare la dibattuta tematica della responsabilità penale delle macchine, che trova attuale sviluppo in relazione alle *self-driving cars* e ai *drone-crimes*.

la collocazione spaziale e fisica è totalmente estranea alla circolazione dei dati in una rete di comunicazione telematica ed alla loro contemporanea consultabilità da parte di più utenti spazialmente diffusi sul territorio[77].

Conseguentemente deve ritenersi che, ai fini della determinazione del *locus commissi delicti* dei reati commessi nel *cyberspace*, rileva esclusivamente il luogo da cui parte il dialogo elettronico tra i sistemi interconnessi ed al quale può conseguire – come nel caso affrontato dai giudici in relazione all'art. 615-*ter* c.p. - l'accesso abusivo nel secondo[78]. Il sistema ove sono archiviati i dati e nel quale si accede abusivamente, invece, è privo di rilevanza, in quanto il criterio della sua collocazione non esaurisce la complessità del trattamento delle informazioni nel *cyberspace*[79].

---

[77] Si ritiene di evidenziare come la soluzione offerta dalle Sezioni Unite presenti interessanti risvolti anche in relazione all'individuazione della legge da applicare al caso in cui l'intrusione sia realizzata dall'estero, nei confronti di un sistema informatico italiano. Con riguardo a tali casi, si è osservato che le caratteristiche del *cyberspace* comportano che la condotta abbia una proiezione che si estende al *server* collegato in Italia. In tal modo, si potrebbe arrivare a sostenere che l'azione criminosa, compiuta dall'operatore senza allontanarsi fisicamente dalla postazione periferica collocata all'estero, sia realizzata, proprio in ragione del carattere immateriale e deterritorializzato della dimensione cibernetica, almeno in parte in Italia, con conseguente applicabilità dell'art. 6, co. 2, c.p. Sul punto GUP Trib. Roma (Giudice d'Alessandro), ord. 16 aprile 2014, nonché M. BELLACOSA, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, op. cit., p. 12 e C. F. GROSSO, *Su di un'interessante controversia interpretativa in tema di luogo del commesso reato e di giudice competente per territorio in materia di accesso abusivo in un sistema informatico*, op. cit.

[78] Cass., pen., SS.UU., sent. 24.4.2015, n. 17325, p. 10: «L'accesso inizia con l'unica condotta umana di natura materiale, consistente nella digitazione da remoto delle credenziali di autenticazione da parte dell'utente, mentre tutti gli eventi successivi assumono i connotati di comportamenti comunicativi tra il client e il server. L'ingresso o l'introduzione abusiva, allora, vengono ad essere integrati nel luogo in cui l'operatore materialmente digita la password di accesso o esegue la procedura di login, che determina il superamento delle misure di sicurezza apposte dal titolare del sistema, in tal modo realizzando l'accesso alla banca dati».

[79] Cass. pen., SS.UU., sent. 24.4.2015, n. 17325, p. 10: «[…] è arbitrario effettuare un'irragionevole scomposizione tra i singoli componenti dell'architettura di rete, separando i terminali periferici dal server centrale, dovendo tutto il sistema essere inteso come un complesso inscindibile nel quale le postazioni remote non costituiscono soltanto strumenti passivi di accesso o di interrogazione, ma essi stessi formano parte integrante di un complesso meccanismo, che e strutturato in modo da esaltare la funzione di immissione e di estrazione dei dati da parte del *client*».

4.2. La ricerca del bene giuridico comune ai reati cibernetici: l'incompatibilità fra cyberspazio e inviolabilità del domicilio

I *cybercrimes* si distinguono dai *reati informatici* anche per il bene giuridico offeso. Tuttavia l'ordinamento italiano - che non prevede la tipizzazione dei reati cibernetici, accontentandosi di disciplinare (senza significativi aggiornamenti) i soli *computer crimes* - ignora i nuovi beni giuridici emersi in relazione allo sviluppo tecnologico, ritenendo (dopo un trentennio) che essi debbano ricondursi all'*integrità del sistema informatico* e *all'inviolabilità del domicilio informatico.*

In questo paragrafo, dunque, si intende, da un alto, dimostrare l'autonomia degli interessi giuridici cibernetici rispetto a quelli informatici e, dall'altro lato, interrogarsi circa l'opportunità di assicurare adeguata tutela penale ai primi.

Procedendo con ordine, giova preliminarmente osservare che il Titolo XII del Libro II del codice penale è dedicato ai *delitti contro la persona*. In particolare la Sezione IV del Capo III del succitato Titolo - la quale contiene la maggior parte dei cosiddetti delitti informatici - raggruppa le fattispecie poste a tutela dell'*inviolabilità del domicilio*. Fra queste sono ricomprese le fattispecie di "*Accesso abusivo ad un sistema informatico o telematico*" (art. 615-*ter* c.p.), "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*" (art. 615-*quater* c.p.) e "*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*" (art. 615-*quinquies* c.p.), che, come ha evidenziato parte della dottrina, sarebbero dedicati alla tutela di una peculiare tipologia di domicilio (cioè quello informatico).

La legge 23.12.1993, n. 547, che ha introdotto complessivamente nove delle fattispecie informatiche attualmente previste dal nostro codice, ha ridisegnando la gamma degli interessi meritevoli di tutela in materia. Tuttavia questi, sebbene siano stati ritenuti concettualmente autonomi da parte della dottrina, non hanno ricevuto espressa positivizzazione nel codice come beni

giuridici di categoria, con risultati non condivisibili sotto un profilo logico, prima ancora che giuridico[80].

Tra gli interessi emersi in relazione all'informatica, assume particolare rilievo il cosiddetto *domicilio informatico*, che, mutuando la definizione di domicilio tradizionale[81], può definirsi come il luogo ideale (un *software* o, più in generale, un sistema informatico o telematico) o anche fisico (un *hardware*) di pertinenza esclusiva di un determinato soggetto, ove si svolgono attività che riguardano dati e informazioni dello stesso - compresa quella di mera raccolta - tali da meritare *riservatezza* ed *inviolabilità*[82]. Detta definizione trova conferma

---

[80] R. FLOR, *Phishing, identity theft, e identity abuse.* op. cit., p. 899, in cui l'autore ritiene che la fattispecie prevista dall'art. 615-*ter* c.p. sia posta a tutela del bene giuridico della riservatezza informatica. Questo consiste nell'interesse a godere, disporre e controllare le informazioni, i procedimenti, i sistemi e gli spazi informatizzati, nonché le relative utilità. In ogni caso rileva osservare che nella Relazione di accompagnamento al d.d.l. n. 2773 del 1993 (che anticipava la l. 23.12.1993, n. 547), si evidenziava come si fosse ampiamente dibattuto con riguardo all'opportunità di modificare il codice penale, prevedendo un apposito titolo per i reati informatici, risultando questa la scelta preferibile originariamente. Tuttavia il legislatore, come noto, ha ritenuto di ricondurre le nuove fattispecie a quelle già esistenti, escludendo che i reati informatici siano caratterizzati da un oggetto giuridico comune «inteso quanto meno come unico interesse di categoria». Infine consta rilevare come già nel d.d.l. n. 5076 del 1990 (presentato nei mesi immediatamente successivi all'adozione della Raccomandazione n. R (89) 9 del Consiglio d'Europa), si prevedesse l'introduzione di una nuova Sezione nel Capo III del Titolo XII del Codice penale, dedicata ai delitti in materia informatica e telematica.

[81] Sul concetto di domicilio penalisticamente rilevante si veda R. GAROFOLI, *Manuale di diritto penale. Parte speciale*, Neldiritto, 2022, p. 197; G. COCCO, E. M. AMBROSETTI, *Trattato breve di Diritto Penale - Parte speciale*, CEDAM, 2021, p. 448; nonché, sotto il profilo della giurisprudenza, C. Cost., sent. 24.4.2002, n. 135. Per un commento della pronuncia si consiglia la lettura di P. VERONESI, *Per un'interpretazione costituzionale del concetto di "domicilio"*, in *Ann. Univ. Ferrara*, XVII, 2003, p. 125.

[82] Del concetto di domicilio informatico vi è traccia anche nella proposta di legge in materia di captatori informatici C. 4260, presentata il 31.1.2017 e recante modifiche al codice di procedura penale e altre disposizioni concernenti la disciplina dell'intercettazione di comunicazioni telematiche e dell'acquisizione di dati ad esse relativi. In particolare la relazione al disegno di legge afferma che: «le captazioni da remoto incidono sull'inviolabilità del domicilio», nel senso di «domicilio informatico, ossia quello spazio immateriale, delimitato da informazioni, nel quale una persona esplica attività legate alla vita privata o di relazione, e dall'accesso al quale il titolare ha diritto di escludere terzi». C. PECORELLA, *Diritto penale dell'informatica*, CEDAM, 2006, p. 32, in cui, conformemente alla dottrina maggioritaria, si ritiene che il bene protetto dalla norma investirebbe l'integrità dei dati e dei sistemi informatici oppure la riservatezza dei dati e dei programmi ivi contenuti. Con particolare riguardo alla riservatezza ed inviolabilità dei dati degli utenti, invece, si veda G. PICA, *Diritto penale delle tecnologie informatiche*, UTET,

nella giurisprudenza della Corte di Cassazione che, nel ritenere il domicilio informatico un'estrinsecazione di quello tradizionale, ne ha individuato il contenuto tipico negli elementi della *riservatezza* e dell'*esclusività*[83].

La concettualizzazione del domicilio informatico, come mera estrinsecazione di quello tradizionale, è stata criticata dalla dottrina occupatasi di distinguere i *computer crimes* dai *cybercrimes*, la quale ne ha escluso l'applicabilità rispetto ai secondi. Essa, infatti, permetterebbe di cogliere solo parzialmente il contenuto dell'*interesse all'esclusione di terzi* nello spazio cibernetico[84].

1999, p. 62, in cui si ritiene che questi interessi potrebbero essere efficacemente garantiti solo accogliendo una concezione restrittiva di domicilio, quale «luogo da mantenere riservato attraverso misure di sicurezza che garantiscano l'esercizio dello *ius excludendi alios*».

[83] Cass. pen., Sez. VI, sent. 4.10.1999, n. 3067; Cass. pen., Sez. V, sent. 26.10.2012, n. 42021; Cass. pen., Sez. V, sent. 31.3.2016, n. 13057, in cui i giudici si sono dimostrati concordi nel ritenere che il contenuto del domicilio informatico «si concreta nello *ius excludendi alios*, quale che sia il contenuto dei dati racchiusi in esso, purché attinenti alla sfera di pensiero o all'attività, lavorativa o non, dell'utente». Concordemente in dottrina C. DOMENICALI, *Tutela della persona negli spazi virtuali: la strada del "domicilio informatico"*, in *Federalismi*, 28.3.2018, p. 18, nota 51, ove si precisa che, in ogni caso, i dati devono attenere alla sfera di pensiero o all'attività - lavorativa o non - dell'utente, non potendosi limitare a quelli personalissimi.

[84] Cosi L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, op. cit., p. 80. Per una definizione approfondita di *cyberspace* si rinvia al precedente paragrafo v. *supra* §. 2 di questo capitolo. Ad ogni modo qui si ritiene di dare conto della definizione di *cyberspace* che la dottrina ha fornito con specifico riferimento alla questione dell'emersione dei nuovi beni giuridici. Sul punto R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*, in *Dir. Pen. Cont*., 2012, pp. 1-2. L'autore sostiene che il *cyberspace* è un luogo in continua evoluzione, la cui natura spazio-temporale non è fisica, tanto che si parla di realtà delocalizzata e detemporalizzata. In esso circolano esclusivamente informazioni, che, sotto il profilo spaziale, sono raggiungibili da ogni dove e a qualsiasi distanza, anche grazie alle nuova dimensione del *cloud* e della "struttura" del *web*. Sotto il profilo temporale, invece, le attività possono essere pianificate e svolte attraverso operazioni automatizzate, programmate dall'utente, senza la necessaria presenza fisica e azione della persona umana. Alla luce di questa definizione, giova osservare che 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* per l'appunto delocalizzate in rete. Con riferimento alle problematiche giuridiche, specificatamente coinvolgenti la tutela dei dati e delle informazioni, legate al *cloud* si veda 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, pp. 117 e ss.; J. SPOENLE, *Cloud Computing and*

Invero la dematerializzazione che connota il *cyberspace* (e quindi i *cybercrimes*), quale «spazio virtuale di manifestazione della personalità», richiede che venga tutelato «l'interesse sostanziale alla protezione di informazioni "riservate" e al loro controllo nello svolgimento di rapporti giuridici e personali *online*» o in altri spazi virtuali. Detta tutela, nel caso dei *cybercrimes*, deve essere assicurata a prescindere dalla collocazione fisica dei sistemi informatici, i quali, come si è detto, non sono elementi essenziali del fatto tipico del reato cibernetico[85].

L'incompatibilità fra il *cyberspace* e le forme di tutela del domicilio tradizionale (che il legislatore ritiene di poter estendere rigidamente agli interessi legati al domicilio informatico[86]) emerge anche in relazione ai criteri dettati dall'ordinamento civilistico in materia di *ius excludendi alios* (art. 14 Cost.), sul quale esse si fondano[87]. Invero tali criteri, che sono sanciti dall'art. 832 c.c. in relazione al contenuto del diritto di proprietà[88], presuppongono l'esistenza di un "confine da violare", che mal si concilia con la natura dematerializzata e sconfinata dello spazio cibernetico, ove non è possibile tracciare un solco che distingua ciò che è privato da ciò che non lo è[89].

---

cybercrime investigations: Territoriality vs. the power of disposal? Discussion paper, Council of Europe, Strasbourg, 2010.

[85] Cosi R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. trim. dir. pen. ec.*, 3/2009, p. 705.

[86] C. LARINNI, *op. cit.*, p. 14.

[87] In Council of Europe, *Final report of the European Committee on Crime problems*, Strasbourg, 1990, pp. 22-24: in cui si legge che «non è possibile, in linea generale, accordare una protezione assoluta ed esclusiva alle informazioni, in termini analoghi al diritto di proprietà» e che, anzi, è necessario «operare un bilanciamento degli interessi contrapposti […] alla luce della tipologia delle informazioni e delle misure di sicurezza impiegate, […] al fine di determinare fino a che punto uno specifico tipo di informazione sia meritevole di protezione». Sul punto C. LARINNI, *op. cit.*, p. 13.

[88] Art. 832 c.c., rubricato "*Contenuto del diritto*": «Il proprietario ha diritto di godere e disporre delle cose in modo pieno ed esclusivo, entro i limiti e con l'osservanza degli obblighi stabiliti dall'ordinamento giuridico».

[89] C. DOMENICALI, *op. cit.*, p. 8; R. ORLANDI, *Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici*, in *Arch. Pen.*, 25.7.2016, pp. 10 e ss., ove la *riservatezza informatica* è definita l'«interesse al godimento e controllo esclusivo sia di determinati dati e informazioni, che dei relativi mezzi e procedimenti informatici e telematici di trattamento». Contestualmente si evidenzia che la riservatezza, pur

La dottrina, attesa l'incompatibilità dei beni giuridici informatici (in particolare dell'inviolabilità del domicilio) rispetto alla cibernetica, ha cercato di definire i nuovi interessi che emergono in relazione al *cyberspace*, ove le esigenze di riservatezza ed esclusività diventano ancora più forti[90].

Secondo alcuni autori l'interesse giuridico rilevante consisterebbe nel binomio «riservatezza e sicurezza informatica», da intendersi come diritto di godere, disporre e controllare le informazioni, i procedimenti, gli ''spazi'' informatizzati e le relative utilità[91]; secondo altri nella libertà personale, la quale - nello spazio cibernetico - consisterebbe nell'«*habeas data*»[92]; secondo altri ancora - mutuando un concetto già emerso nel diritto penale tedesco –

---

configurandosi come «diritto di escludere» i terzi non legittimati dal corrispondente accesso e utilizzo, va oltre la dimensione originaria della tutela del domicilio. Pertanto pare doversi ritenere non condivisibile la tesi di chi (ad esempio F. BERGHELLA, R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, op. cit., p. 2333) ritiene che la tutela della «fruizione indisturbata» del sistema informatico possa ricondursi a quella del «pacifico godimento della proprietà fondiaria». Infatti il concetto di sistema informatico non può essere ridotto a quello di luogo privato, né a quello di mera proiezione virtuale del domicilio penalmente rilevante, per due principali ragioni. La prima attiene alla circostanza che, come detto, i contenuti del sistema informatico non sempre - ed anzi solo in un numero estremamente esiguo di casi – presentano carattere strettamente personale, che, invece, è essenziale rispetto al domicilio e ai luoghi di privata dimora. La seconda ragione attiene all'aspetto sanzionatorio. Invero, confrontando l'art. 615-*ter* c.p. e, ad esempio, l'art. 637 c.p. (rubricato "*Ingresso abusivo nel fondo altrui"*), emerge una sensibile differenza circa la pena: fino a tre anni di reclusione in caso di accesso abusivo ad un sistema informatico e multa fino ad euro 103 per l'ingresso abusivo nel fondo altrui. Ciò evidentemente contribuisce ad escludere l'assimilabilità fra i due concetti. Alla stessa conclusione conducono anche le differenze in punto di procedibilità: per l'art. 637 c.p. sempre a querela della persona offesa; per l'art. 615-*ter* c.p. solo nel caso di cui al relativo comma 1.

[90] R. FLOR*, ibidem*, p. 705, in cui l'autore evidenzia come la matrice del nuovo *diritto alla riservatezza ed esclusività* - pur sempre rappresentata dall'esigenza di riservatezza del titolare e quindi dallo *ius excludendi alios* - si spinga oltre la dimensione originaria della *privacy* e della tutela del domicilio, anche se inteso in senso informatico.

[91] L. PICOTTI*, Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, op. cit., pp. 21 e ss.; R. FLOR, *Phishing, identity theft, e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. It. dir. e proc. pen.*, 2007, p. 899; P. VENEZIANI, *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in *Ind. Pen*., 1/2000, p. 139.

[92] S. RODOTÀ, *Discorso del Presidente Stefano Rodotà*, nella *Relazione annuale del Garante della Privacy*, 2004, p. 16. L'autore ritiene opportuno che la libertà personale venga garantita anche nel *cyberspace*. Nella dimensione depersonalizzata e dematerializzata gli utenti rilevano come fasci di dati e informazioni, che devono essere tutelati alla stregua di proiezioni della libertà personale.

nell'«autodeterminazione informativa», come libertà di trattare e gestire le proprie informazioni[93].

A ben vedere, ciascuno degli interessi summenzionati riguarda una delle componenti del *cyberspace* (secondo la struttura tripartita dello steso, elaborata da Even e Siman-Tov).

Più nello specifico, la *sicurezza* e la *riservatezza informatiche* attengono al *physical layer*, ovverosia lo strumento necessario per "trasferirsi" dalla dimensione reale a quella virtuale. L'*habeas data*, invece, rileva in relazione al *logical layer*, cioè all'insieme dei dati trasmessi e trattati nel *cyberspace*. L'*autodeterminazione informativa*, infine, riguarda più direttamente lo *human layer*, ovverosia la componente umana dello spazio cibernetico, alla quale deve

---

[93] Trattasi del *Recht auf informationelle Selbstbestimmung*. Per la definizione giurisprudenziale di «autodeterminazione informativa», cfr. BVerfG, sent. 15.12.1983 (1 BvR 209/83), in cui i giudici tedeschi, riconoscendole natura di diritto fondamentale a cui attribuire rilievo costituzionale, evidenziano che: «L'autodeterminazione pertanto deve essere tutelata nel contesto delle attuali e future condizioni di trattamento automatico di grandi quantità di dati. Questa facoltà, infatti, risulta attualmente in pericolo poiché nei processi decisionali non si deve più, come accadeva in passato, ricorrere a schedari e ad atti raccolti manualmente, ma, con l'aiuto dell'elaborazione automatica dei dati, informazioni relative a circostanze personali o intime di una persona identificata o identificabile sono tecnicamente visibili, memorizzabili senza limitazioni e accessibili in pochi secondi (a prescindere dal luogo in cui si trovano) (art. 2 co. 1, *Bundesdatenschutzgesetz*). Inoltre questi dati possono essere combinati con altre banche dati contenenti profili della personalità parziali o quasi completi, in particolare attraverso la costruzione di sistemi informativi integrati, senza che gli interessati possano verificarne in modo sufficiente la correttezza e l'utilizzo che ne viene fatto. Con la costruzione di questi sistemi informativi integrati sono state ampliate in modo inimmaginabile le possibilità di controllo e condizionamento delle istituzioni sui cittadini, circostanza che influisce sul comportamento dei singoli in quanto gli stessi sono portati a subire una pressione psicologica da parte dello Stato. L'autodeterminazione presuppone, anche nel contesto delle moderne tecnologie per il trattamento delle informazioni, che ai singoli individui sia data la libertà di decidere (Entscheidungsfreiheit) se scegliere di intraprendere o di rinunciare a determinate attività, compresa la possibilità di comportarsi di conseguenza […]. Da ciò consegue che: il libero sviluppo della personalità umana, nel moderno contesto del trattamento dei dati, presuppone la tutela dei singoli contro la raccolta, memorizzazione, utilizzazione e trasferimento senza limitazioni dei suoi dati personali. Questa tutela è perciò ricompresa nel diritto fondamentale di cui agli artt. 2, co. 1, e 1, co. 1, della Costituzione». Per una definizione dottrinale, invece, si veda S. SIMITIS, *Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung*, in *NJW*, 8/1984.

essere garantita la libertà di gestire autonomamente le proprie informazioni e di usare il *cybespace*.

Ebbene, chi scrive ritiene che gli interessi individuati dalla dottrina debbano essere ricondotti *ad unum* - al fine di evitare un'eccessiva frammentazione di tutela - ed individuare un unico bene giuridico di categoria comune ai *cybercrimes*, che assommi in sé tutti i predetti interessi

L'ordinamento italiano non contempla un bene giuridico di simile portata. Diversamente il diritto eurounitario offre interessanti spunti di riflessione sul tema. Per tali ragioni, nel prossimo paragrafo, si esaminerà la normativa europea di riferimento in un'ottica comparatistica, al fine di vagliare se, a livello sovranazionale, sia individuabile un bene giuridico comune ai *cybercrimes*.

4.3. L'evoluzione della tutela degli interessi giuridici connessi alle tecnologie dell'informazione nel diritto europeo: la cybersicurezza come bene giuridico offeso dai cybercrimes

Il diritto europeo, diversamente da quello domestico, ha dimostrato grande interesse per le interazioni fra diritto e nuove tecnologie, occupandosi di individuare gli interessi giuridici che emergono in relazione all'uso delle stesse.

In particolare, con il regolamento (CE) n. 460/2004, istitutivo dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), il legislatore europeo ha riconosciuto piena autonomia alla *sicurezza informatica*. Questa, a norma dell'art. 4, lett. c del regolamento in parola è: «la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei relativi servizi forniti o accessibili tramite tale rete o sistema». Tra i principali compiti dell'ENISA, figura proprio l'elaborazione di metodologie comuni al fine di prevenire, affrontare e risolvere le minacce rivolte alla sicurezza delle reti e dell'informazione (art. 3, lett. d).

La direttiva (UE) 2016/1148 (recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione), poi, ha predisposto un complesso sistema di tutele volto a garantire la *sicurezza della rete e dei sistemi informativi*. In particolare la direttiva prescrive agli Stati di istituire appositi gruppi di intervento contro gli incidenti che possono interessare le reti (CSIRT) e di promuovere la cultura della sicurezza nei settori basati sulle tecnologie dell'informazione e della comunicazione[94].

Il legislatore nazionale non sembra non aver compreso l'importanza dei nuovi interessi giuridici emersi in relazione alle nuove tecnologie, ritenendo superfluo attribuirgli rilievo costituzionale e qualsivoglia forma di tutela penale. Sul punto si ricorda che – a tacere della lacuna in materia di reati cibernetici – il legislatore colloca il gruppo più significativo dei reati informatici nella Sezione IV del Titolo XII del Libro II del codice penale, dedicata ai delitti contro l'inviolabilità del domicilio.

Diversamente, la giurisprudenza di altri Paesi europei si è conformata all'impostazione sovranazionale, riconoscendo la necessità di tutelare in via autonoma i nuovi interessi giuridici emersi in relazione alla cibernetica.

In proposito, meritano di essere esaminate le conclusioni a cui è pervenuto il *Bundesverfassungsgericht* nella sentenza del 27.2.2008, n. 370/07.

La Corte costituzionale federale tedesca - chiamata a pronunciarsi in tema di monitoraggio occulto di un sistema informatico - ha statuito che, per assicurare adeguata tutela ai nuovi interessi giuridici legati alla cibernetica, fosse insufficiente estendere la portata applicativa delle garanzie, già previste nella

---

[94] In particolare la direttiva (art. 2, par. 2): a) fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi; b) istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi; c) crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace; d) stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali; e) fa obbligo agli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi.

Costituzione tedesca in materia di *segretezza delle telecomunicazioni*, *inviolabilità del domicilio* e *autodeterminazione informativa*, attraverso un mero correttivo di carattere interpretativo. Invero la Corte Costituzionale ha ritenuto indispensabile un intervento del legislatore, il quale, infatti, ha provveduto ad introdurre il nuovo diritto costituzionale all'«integrità ed alla riservatezza dei sistemi informatici» (*ex* art. 1, co. 1, e art. 2, co. 1, GG) [95].

Più recentemente, il Regolamento (UE) 2019/881 del 17.4.2019 (relativo ai compiti dell'ENISA e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione) – alle luce dello sviluppo delle nuove tecnologie cibernetiche - ha superato il concetto di sicurezza informatica, introducendo la nozione di «cybersicurezza»[96]. Questa a norma dell'art. 2, n. 1 del summenzionato regolamento è intesa come la *protezione della rete e dei sistemi informativi, degli utenti di tali sistemi e delle altre persone interessate dalle minacce cibernetiche*.

Il concetto di *cybersicurezza*, dunque, è più ampio rispetto a quello di *sicurezza informatica*, per almeno due ragioni. Sotto un primo profilo, esso tutela utenti e persone – ammettendo che possano essere destinatari di offese nel *cyberspace* – e non soltanto sistemi e dati informatici. Sotto un secondo profilo, poi, la *cybersicurezza* non interessa soltanto gli utenti dei sistemi informatici, ma

---

[95] BVerfG, Z.S., sent. 27.2.2008, 370/07. Sul punto si veda R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung,* op. cit., 3/2009, p. 705, in cui l'autore spiega che la Corte era chiamata a valutare la legittimità di una norma della legge sulla protezione della Costituzione del Nord Reno-Westfalia, perché consentiva ad un organismo di *intelligence*, di derivazione governativa, il monitoraggio e l'accesso segreto ai sistemi informatici collegati in rete. Inoltre, per riferimenti dottrinali che condividono la necessità dell'introduzione di nuovi beni giuridici, valorizzando la citata giurisprudenza teutonica si veda M. TORRE, *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali,* in *Dir. Pen. e Proc.,* 9/2015, pp. 1163 e ss. e D. DOMENICALI, *op. cit.*, p. 9, in cui emerge che il nuovo diritto deve intendersi espressione della tutela della dignità dell'uomo, come utente informatico o «cittadino digitale» nell'uso delle tecnologie di informazione e di comunicazione in rete.

[96] Regolamento (UE) 2019/881 relativo ai compiti dell'ENISA (Agenzia dell'Unione europea per la cybersicurezza) e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione.

anche tutte le persone che, pur sprovviste di detta qualifica, sono a vario titolo interessate dalle minacce cibernetiche.

A bene vedere, il concetto europeo di cybersicurezza è in grado di ricomprendere la «*sicurezza* e *riservatezza informatiche*», l'«*habeas data*» e l'«*autodeterminazione informativa*» che - come si è detto nel precedente paragrafo - la dottrina ha indicato come interessi offesi dai reati cibernetici e, pertanto, rappresenta il bene giuridico comune ai reati cibernetici. In particolare, esaminando la definizione europea emerge che: la *protezione della rete e dei sistemi informativi* afferisce al primo dei tre interessi; la tutela degli utenti e delle altre persone (destinatarie di minaccia), invece, attiene agli ultimi due, con la notazione che la cybersicurezza non tutela soltanto la libertà di gestire i propri dati e di usare liberamente il cyberspazio (secondo l'impostazione finora adottata in relazione ai *computer crimes*), ma investe anche l'integrità fisica e psichica dei soggetti, che può dunque essere direttamente offesa dai *cybercrimes*[97].

5. Il cyberterrorismo: nascita del concetto e primi tentativi definitori

Il cyberterrorismo è il *cybercrime* che presenta il maggior grado di disvalore penale, attesi i beni giuridici offesi e le caratteristiche della condotta rilevante. Nonostante la rapida evoluzione che il fenomeno in parola ha conosciuto negli ultimi anni[98], attualmente non esiste una definizione condivisa a livello internazionale di terrorismo cibernetico, né tantomeno una fattispecie astratta che ne offra una tipizzazione a livello domestico.

Tali lacune hanno indotto gran parte della dottrina a ritenere che la disciplina del cyberterrorismo debba ricavarsi dalla mera giustapposizione delle

---

[97] BRIGHI R., CHIARA P. G., *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi*, 8.9.2021, pp. 18-42.

[98] V. *supra* nota 8.

norme dettate in materia di terrorismo, da un lato, e di quelle relative ai reati informatici, dall'altro[99].

Tuttavia tale scelta ermeneutica presta il fianco ad almeno due critiche.

Sotto un primo profilo, si continua a fare riferimento ai reati informatici, i quali, come s'è detto precedentemente, sono inadeguati – a distanza di un trentennio dalla loro introduzione nel nostro ordinamento, ad opera della l. 23.12.1993, n. 547 - a descrivere le novità della cibernetica.

La seconda critica, invece, attiene al concetto stesso di *terrorismo* ed alla relativa disciplina. Infatti se, da un lato, è incontrovertibile che il cyberterrorismo sia un reato connotato dalla *finalità di terrorismo* (art. 270-*sexies* c.p.), dall'altro lato, si rende necessario verificare se l'attuale disciplina italiana in materia di *terrorismo comune* sia *tout court* applicabile al nuovo fenomeno, anche atteso che, a tutt'oggi, non esiste una definizione di terrorismo trasversalmente condivisa. Tali incertezze rendono necessaria un'indagine circa le caratteristiche

---

[99] L'impostazione in parola qualifica il cyberterrorismo come un fenomeno *tool-oriented*. Tale espressione descrive il legame intercorrente fra la rete (*rectius* il *cyberspace* e più in generale la cibernetica) ed il terrorismo alla stregua di un mero rapporto di strumentalità, di talché il cyberterrorismo non sarebbe altro che la realizzazione di condotte terroristiche mediante il mezzo informatico. Per un esame dell'approccio *tool-oriented*, si rinvia a F. VIGNERI, *Cyberterrorismo: realtà o finzione?*, op. cit., p. 13; A. M. TALIHÄRM*, Cyberterrorism: in theory or in practice?*, in *Defence Against Terrorism Review*, 2/2010, pp. 63-64; M. C. DE VIVO, G. RICCI, *Diritto, crimini e tecnologie*, in *Informatica e diritto*, 2/2012, p. 14, in cui gli autori definiscono il cyberterrorismo come «reato commesso con l'uso del pc»; P. M. SABELLA, *Il fenomeno dei cybercrimes nello spazio giuridico contemporaneo*, *op. cit.*, pp. 139-176; G. ILARDA, G. MARULLO, *Cybercrime: conferenza internazionale*, Giuffrè, 2004, pp. 133 e ss. Ad ogni modo l'approccio *tool-oriented* – che chi scrive non ritiene condivisibile – è conforme all'impostazione del legislatore italiano in materia di *cybercrimes* (che si è ampiamente criticata nei paragrafi precedenti di questo Capitolo), il quale ha qualificato come aggravante – e non invece come autonoma fattispecie di reato – l'utilizzo degli strumenti informatici (e comunque, si badi, non cibernetici) per la realizzazione di particolari condotte con finalità di terrorismo. Ci si riferisce peculiarmente alla fattispecie di "*Addestramento ad attività con finalità di terrorismo anche internazionale*" (art. *quinquies* c.p.), introdotta con d.l. 27.7.2005, n. 144 (conv. in l. 31.4.2005, n. 155), che al suo secondo comma (aggiunto *ex* art. 1, co. 3, lett. b, d.l. 7/2015, conv. in l. 43/2015, n. 43, c.d. *Decreto antiterrorismo*) recita: «Le pene per il presente articolo sono aumentate se il fatto di chi addestra o istruisce è commesso attraverso strumenti informatici o telematici». Per un'interpretazione del cyberterrorismo nel senso di aggravante, S. COLAIOCCO, *Le nuove norme antiterrorismo e le libertà della persona: quale equilibrio?*, in *Arch. pen*., 2/2015, p. 5; S. CENTONZE, L. GIOVEDI, *Terrorismo e legislazione d'emergenza*, Key, 2016, pp. 181 e ss.

del reato di *terrorismo comune*, soffermandosi sui relativi elementi costitutivi, onde disporre di tutti gli strumenti concettuali per chiarire il rapporto che lo lega alla cibernetica.

Ad ogni buon conto, il concetto di cyberterrorismo è stato elaborato dal ricercatore californiano Barry Collins attorno alla prima metà degli anni '80 del secolo scorso, il quale ne ha proposto la seguente definizione: «the intentional abuse of a digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action»[100].

Secondo Collins, il *cyberterrorism*, sotto il *profilo oggettivo*, si configura come l'*impiego abusivo di un sistema di informazione digitale* (si noti come non venga utilizzato l'obsoleto concetto di informatica), di un *network* o di una loro parte. Il carattere *abusivo* della condotta interesserebbe, dunque, sia l'accesso al sistema, sia il suo utilizzo, qualora l'agente vi si introduca senza autorizzazione o, ancorché disponendo della stessa, se ne avvalga per compiere atti diversi da quelli normalmente ammessi.

Sotto il *profilo soggettivo*, invece, si richiede la finalità di supportare o facilitare azioni o compagne terroristiche. In particolare l'aggettivo «*intentional*» rivelerebbe la necessità che il soggetto agente sia animato quantomeno dal *dolo diretto*, secondo la classificazione prevista nel nostro ordinamento.

La definizione di Collins si dimostra poco condivisibile perché descrive il *cyberterrorism* come giustapposizione fra cibernetica e terrorismo – la prima legata da un rapporto di mera strumentalità al secondo –, ritenendo il sistema di informazione digitale elemento essenziale del fatto tipico (riproducendo sostanzialmente la struttura dei *computer crimes* descritta nel §. 4 di questo Capitolo).

A partire dagli anni '90 del secolo scorso, alcuni autori hanno sostenuto la necessità di elaborare una definizione di cyberterrorismo quanto più ampia

---

[100] P. FLEMING, M. STOHL, *Myths and Realities of Cyberterrorism*, *paper* per l'*International Conference on Countering Terrorism Through Enhanced International Cooperation*, 22.9.2000, p. 30, disponibile al *link*: *http : / / www . comm . ucsb . edu / faculty / mstoh l / Myths % 20and % 20Realities % 20of % 20Cyberterrorism . pdf.*

possibile, al fine di disporre di uno strumento elastico da adattare a tutte le manifestazioni del fenomeno[101]. Detta impostazione è stata critica da coloro che ritenevano imprescindibile il rispetto del principio di determinatezza, richiedendo l'elaborazione di una fattispecie che esplicitasse chiaramente tutti i presupposti necessari per l'integrazione del delitto, al fine di facilitare l'attività sussuntiva dell'interprete[102].

Tra i due orientamenti, il secondo risultava maggioritario, annoverando tra i sostenitori Mark M. Pollitt, già direttore del *Regional Computer Forensic Laboratory Program* dell'FBI (RCFLP)[103], il quale definiva il *cyberterrorism* come: «the premeditated, politically motive attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by subnational groups or clandestine agents»[104].

---

[101] E. LUIIJF, *Definitions of Cyber Terrorism*, in B. AKHAGAR, A. STANIFORTH, F. BOSCO, *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Elviser Science, 2014, p. 11, in cui l'autore spiega come il cyberterrorismo, in accordo a questo orientamento, dovesse intendersi nel senso di «convergence of cybernetics and terrorism»; E. R. PURDY, *Cyberterrorism,* Salem Press Encyclopedia, 2019, pp. 10 e ss., in cui l'autore evidenzia come fosse stata accolta la concezione secondo cui il cyberterrorismo consistesse in «illegal and highly damaging attacks that target computers, networks, and digitally stored information for the purpose of causing harm to people or property or generating fear», secondo una definizione che non consente di evidenziare i tratti distintivi, sotto il profilo oggettivo, del fenomeno rispetto ai *cybercrimes* comuni.

[102] A sostegno di questo orientamento, E. D. DENNING, *Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, in J. ARQUILLA, D. RONFELDT, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defence Research Institute RAND, 2001, pp. 289-288, disponibile al seguente *link*: *https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf*.; M. POLLIT, *Cyberterrorism- Fact or Fancy?*, in *Computer Fraud & Security*, 8/1997, pp. 8-10; M. KENNEY, *Cyber-Terrorism in a Post-Stuxnet World*, Orbis, 2015, p. 112, in cui l'autore sostiene che il cyberterrorismo deve considerarsi appartenente al *genus* dei *cybercrimes*, rispetto ai quali tuttavia si differenzia in ragione di alcuni elementi essenziali. L'autore fornisce dunque la seguente definizione: «Intentional access to systems, websites, and/or data without authorization or having exceeded authorized access, and/or the intentional interference with the functioning and/or accessibility of systems, websites, and data without authorization or having exceeded authorized access, in order to effect social or political change».

[103] Si tratta di un programma che vede la collaborazione tra FBI e altre forze dell'ordine (federali, statali e locali) degli Stati Uniti per la gestione di una *task force* volta a contrastare *computer crimes* e *cybercrimes* su base regionale.

[104] M. POLLIT, *Cyberterrorism- Fact or Fancy?*, op. cit., p. 8.

Per quanto riguarda i *soggetti attivi del reato*, Pollit ritiene che le condotte di terrorismo cibernetico siano poste in essere da gruppi "subnazionali" o da agenti "clandestini". In ogni caso soggetto agente del reato non può essere lo Stato, atteso che in un caso siffatto le azioni poste in essere sarebbero da considerare atti di guerra.

Per quanto attiene all'*elemento oggettivo*, invece, la condotta rilevante - che deve essere violenta - può consistere in un attacco contro informazioni, dati o sistemi informatici.

Infine, per quanto attiene al *profilo soggettivo*, Pollit sostiene che il reato debba essere «*premeditated*», postulando cioè la preordinazione di mezzi e modalità per la realizzazione di un piano criminoso, con significativo lasso di tempo tra le fasi di ideazione e concreta attuazione.

A seguito della virata cibernetica della rivoluzione informatica, registratasi sul finire degli anni '90 dello scorso secolo, anche le più importanti Organizzazioni sovranazionali si sono occupate del *cyberterrorism*, pur senza fornirne una definizione.

Le Nazioni Unite, con la Risoluzione n. 51/210 dell'Assemblea Generale del 16 gennaio 1997 (dedicata al contrasto del terrorismo), hanno ufficialmente preso atto dell'esistenza di un: «risk of terrorists using electronic or wire communications systems and networks to carry out criminal acts» e della necessità di: «to find means, consistent with national law, to prevent such criminality and to promote cooperation where appropriate»[105].

Nello stesso periodo anche il diritto europeo si è occupato, per la prima volta, del *cyberterrorism*. La Commissione europea, con il *memorandum* esplicativo del 19 settembre 2001 sulla proposta della decisione-quadro 2002/475/GAI, ha messo in guardia le Istituzioni europee circa la manifestazione

---

[105] United Nation General Assembly, *Measures to eliminate international terrorism: resolution adopted by the General Assembly A/RES/51/210*, 16.1.1997 (testo disponibile al *link*: *https://www.refworld.org/docid/49997ae127.html*). Rileva evidenziare che nella Risoluzione si fa riferimento all'utilizzo di sistemi di comunicazione e *networks* da parte dei terroristi per il generico compimento di atti criminali, senza null'altro precisare.

delle nuove forme di terrorismo. Contestualmente è stata denunciata l'inadeguatezza delle tradizionali misure normative, relative alla cooperazione giudiziaria e di polizia in materia penale, per contrastare e prevenire efficacemente il nuovo fenomeno[106].

Ad ogni modo la prima definizione di *cyberterrorism*, che possa dirsi completa (sebbene ancora scarsamente connotata sotto il profilo giuridico), risale al 2000 ed è stata formulata da Dorothy Denning[107], secondo la quale il esso consiste in: «*The convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the informations stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not*»[108].

Il cyberterrorismo viene descritto come la "convergenza" tra il terrorismo ed il *cyberspace*, i quali sono entrambi elementi essenziali del fatto tipico, secondo un rapporto paritario e non, invece, strumentale. Invero il *cyberspace* surclassa il concetto di sistema informatico, di cui infatti non v'è traccia nella definizione. Tale scelta denota la piena consapevolezza circa le accresciute potenzialità offerte ai terroristi dalla cibernetica.

Per quanto attiene all'*elemento oggettivo* del reato, l'autrice ritiene che la condotta, pur sostanziandosi in attacchi (o minacce di attacco) contro *computers*, reti, o informazioni, presenti un *quid pluris* rispetto a quanto teorizzato in

---

[106] Sul punto U. SIEBER, *International cooperation against terrorist use of the Internet*, in *Eres*, 3/2006, pp. 395-449.

[107] Professoressa di *information security* presso il *Department of Defense Analysis della Naval Postgraduate School* di Monterey (California).

[108] D. E. DENNING, *Cyberterrorism*, Georgetown University, 2000, pp. 10 e ss.

precedenza, ovverosia l'*idoneità ad ingenerare uno stato di paura nella popolazione dello Stato colpito*[109]. Inoltre Denning precisa che il danno cagionato dal cyberterrorismo deve essere *grave* ed indirizzato *contro le infrastrutture critiche di un Paese*, non rilevando gli attacchi rivolti ai servizi non essenziali dello Stato.

La definizione in esame presenta significative novità anche in relazione all'elemento psicologico del reato. Invero il cyberterrorista deve essere animato dal *dolo specifico* di costringere il Governo (inteso quale struttura istituzionale) o la popolazione dello Stato a compiere delle scelte, in ambito politico o sociale, diverse da quelle che verrebbero altrimenti assunte attraverso il metodo democratico.

Nel 2004, gli esperti del *Federal Bureau of Investigation* statunitense (FBI) proponevano un'ulteriore definizone di terrorismo cibernetico: «*A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing, confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda*»[110].

Tralasciando il riferimento ai computers e più in generale al sistema informatico – che, diversamente da quanto ritiene Denning, tornano a partecipare del fatto tipico del reato – la definizione contiene alcune rilevanti precisazioni in merito allo *scopo del cyberterrorismo*.

Questo consisterebbe nell'ingenerare paura, confusione o incertezza nella popolazione dello Stato colpito – attraverso non meglio precisate attività subdolamente persuasive (in ogni caso diverse dai classici attentati dinamitardi) -

---

[109] Il requisito oggettivo dell'idoneità ad ingenerare paura nella popolazione dello Stato colpito ha la funzione di delimitare il concetto di cyberterrorismo, evitando di ricomprendervi anche *politically motivated hacking actions*, le quali, pur essendo reati politici che offendono la Personalità dello Stato, non postulano il requisito suddetto.

[110] H. M. HENDERSHOT, *CyberCrime 2003 – Terrorists' Activity in Cyberspace*, *briefing slides from the Cyber Division*, *Briefing slides from the Cyber Division, Federal Bureau of Investigation* (FBI), 6.4.2004, disponibile al link: *http://www.4law.co.il/L373.pdf*.

con lo specifico obiettivo di condizionare il Governo di un Paese o la popolazione stessa nel compimento di scelte che involgono interessi politici, sociali o ideologici[111].

Ebbene, il cyberterrorismo si distingue dal terrorismo comune proprio per questo particolare scopo ulteriore, ovverosia condizionare subdolamente le scelte politiche dei cittadini e di riflesso la politica dello Stato al quale gli stessi appartengono, attraverso l'uso abusivo delle tecnologie cibernetiche.

Conclusivamente, è possibile notare come gli autori cimentatisi nella descrizione del cyberterrorismo abbiano attribuito centralità alla componente tecnica del fenomeno senza valorizzare adeguatamente quella terroristica, con l'effetto di elaborare delle definizioni sostanzialmente prive di contenuto giuridico. Siffatta scelta implica l'acritica accettazione della qualificazione del cyberterrorismo alla stregua di mera manifestazione alternativa del terrorismo comune.

Nel presente lavoro, invece, si ritiene indispensabile esaminare le caratteristiche delle condotte con finalità di terrorismo (sia sotto il profilo oggettivo che oggettivo), al fine di vagliare se la disciplina che le riguarda sia *tout court* applicabile al cyberterrorismo o se, invece, questo fenomeno presenti delle peculiarità – si pensi, in particolare al suesposto ulteriore fine - tali da renderne necessaria un'apposita regolamentazione.

---

[111] E. LUIIJF, *Definitions of Cyber Terrorism*, *op. cit*., p.12, in cui l'autore elabora una definizione sostanzialmente conforme a quella dell'FBI (ivi, p. 16): «*The use, making preparations for, or threat of action designed to cause a social order change, to create a climate of fear or intimidation amongst (part of) the general public, or to influence political decision-making by the government or an international governmental organisation; made for the purposes of advancing a political, religious, racial or ideological cause; by affecting the integrity, confidentiality, and/or availability of information, information systems and networks, or by unauthorised actions affecting information and communication technology based control of real-world physical processes; and it involves or causes: violence to, suffering of, serious injuries to, or the death of (a) persons(s); serious damage to a property; a serious risk to the health and safety of the public; a serious economic loss; a serious breach of ecological safety; a serious breach of the social and political stability and cohesion of a nation*».

6. Il terrorismo: etimologia ed evoluzione storica

La parola «terrorismo», sotto il profilo etimologico, affonda le proprie origini nel verbo latino *terrĕo*, che significa «far tremare», nel senso di «infondere paura», «impaurire»[112]. *Terrĕo*, a sua volta, è caratterizzato dalla radice *ter-*, che nella lingua latina era impiegata per indicare *il moto da luogo*, cioè il movimento di cose o di persone da una posizione ad un'altra e quindi, in senso figurato, uno stato di agitazione[113]. Tale idea sembrerebbe riferirsi, dunque, ad un archetipico concetto di paura verso tutto ciò che si pone in contrasto con la stabilità dell'*ordine precostituito*.

I predetti rilievi etimologici trovano riscontro nelle ragioni sociali e culturali che animano il moderno terrorismo, il quale, a partire dal secondo dopoguerra, è diventato lo strumento sistematicamente impiegato (a livello internazionale) per la commissione dei reati politici[114]. A partire dalla fine degli '80 del secolo scorso, con la caduta del muro di Berlino e gli effetti della globalizzazione, il terrorismo ha mutato base motivazionale e scopi, puntando al condizionamento delle scelte politiche ed economiche dei Governi. L'abbattimento ideale delle frontiere nazionali e l'indebolimento della sovranità degli Stati[115] ha consentito al terrorismo di proporsi nello scenario internazionale come vero e proprio soggetto geopolitico, capace di ricattare singoli Paesi e

---

[112] L. CASTIGLIONI, S. MARIOTTI, *IL - Vocabolario della lingua latina*, Loescher, 1979, sub *terrĕo, ĕs, terrŭi, terrĭtum, ēre*, p. 1466.

[113] La voce "*Terrore"*, in Vocabolario TRECCANI *online*, consultabile al *link*: *https://www.treccani.it/vocabolario/terrore*.

[114] Sul punto si pensi, solo a titolo esemplificativo, agli atti di terrorismo commessi durante la "guerra fredda", nonché al complesso contesto sociale e politico che ha interessato l'Italia tra gli anni '60 e '80 dello scorso secolo. Per un esame di quel periodo storico I. MONTANELLI, M. CERVI, *L'Italia degli anni di piombo*, in I. MONTANELLI (a cura di), *Storia d'Italia*, Vol. XIX, BUR, 2022. Per un esame delle misure di contrasto e prevenzione del terrorismo approntate dal legislatore italiano durante i cosiddetti *anni di piombo* si consiglia la lettura di A. BARAVELLI, *Per una storia della risposta penale al terrorismo italiano (1976-82),* Meridiana, 2020, pp. 73–88.

[115] A. CARRINO, *Kelsen e il problema della Sovranità*, Ed. Sc. It., 1990, pp. 25 e ss.

Organizzazioni sovranazionali[116]. Con l'inizio del corrente secolo, segnato dall'attentato al *World Trade Center* dell'11 settembre 2001, il terrorismo ha ulteriormente mutato le sue finalità e sinanco le sue forme di manifestazione. Per circa due decenni i terroristi hanno compiuto violente stragi, per motivi asseritamente religiosi, al fine precipuo di alimentare un terrore di massa e colpendo, perlopiù casualmente, obbiettivi del tutto generici. Tuttavia, a seguito della sconfitta del cosiddetto *Islamic State* nel 2017, ha preso avvio il nuovo corso del terrorismo, che - accantonato il movente religioso - ha rivendicato con forza la sua natura politica. I terroristi non ritengono più necessario disporre di uno Stato territoriale, preferendo usare il *cyberspace* come nuova dimensione ove porre in essere le loro condotte. In proposito si pensi all'impiego dei *social networks* per propagandare espressamente ideali estremistici, radicalizzare o addestrare. Il terrorista 2.0 è in grado di profilare gli ignari cybernauti - carpendone dati sensibili, interessi, orientamenti, paure - al fine di condizionarne subdolamente le scelte politiche, economiche, culturali e sociali. Il perseguimento di un siffatto scopo incide, alterandolo, sul regolare svolgimento del metodo democratico – che è l'essenza della Personalità dello Stato costituzionale - arrecando così grave danno al Paese al quale gli utenti di internet appartengono.

6.1. La definizione europea di reato terroristico

La definizione europea di reato terroristico è prevista dall'art. 1 della decisione-quadro 2002/475/GAI del 13 giugno 2002, rubricato "*Reati terroristici e diritti e principi giuridici fondamentali*". La disposizione, dopo aver chiarito che il reato terroristico è un atto intenzionale connotato - per *natura* o *contesto* - dall'idoneità d'arrecare grave danno ad un Paese o ad un'organizzazione internazionale, ne tipizza le *finalità* e le *condotte*.

---

[116] A. F. VIGNERI, *Cyberterrorismo: realtà o finzione?*, op. cit., pp. 8 e ss.

Le prime possono consistere alternativamente nell'*intimidazione in modo grave della popolazione*, nell'*indebita costrizione dei poteri pubblici (o di un'organizzazione internazionale) a compiere o astenersi dal compiere un qualsiasi atto*, nella *destabilizzazione in modo grave delle strutture politiche fondamentali (costituzionali, economiche o sociali) di un Paese (o di un'organizzazione internazionale)* o nella *distruzione delle stesse*.

Tra le condotte rilevanti per l'integrazione del terrorismo, invece, figurano gli *attentati alla vita di una persona che possono causarne il decesso e quelli all'integrità fisica di una persona purché gravi*; il *sequestro di persona e cattura di ostaggi*; la *distruzioni di vasta portata di strutture governative o pubbliche, sistemi di trasporto, infrastrutture, compresi i sistemi informatici, piattaforme fisse situate sulla piattaforma continentale ovvero di luoghi pubblici o di proprietà private che possono mettere a repentaglio vite umane o causare perdite economiche considerevoli*; il *sequestro di aeromobili o navi o di altri mezzi di trasporto collettivo di passeggeri o di trasporto di merc*i; la *fabbricazione, detenzione, acquisto, trasporto, fornitura o uso di armi da fuoco, esplosivi, armi atomiche, biologiche e chimiche, nonché, per le armi biologiche e chimiche, ricerca e sviluppo*; la *diffusione di sostanze pericolose, il cagionare incendi, inondazioni o esplosioni i cui effetti mettano in pericolo vite umane*; la *manomissione o interruzione della fornitura di acqua, energia o altre risorse naturali fondamentali il cui effetto metta in pericolo vite umane*[117].

Nella decisione-quadro 2008/919/GAI del 28.11.2008, modificativa della precedente, il legislatore europeo ha dimostrato attenzione per le nuove forme di terrorismo, in particolare quelle informatiche. Invero nel Considerando n. 3 della decisone-quadro, per la prima volta, viene fatto espresso riferimento ad un rinnovato «*modus operandi* di attivisti e sostenitori del terrorismo» e alla diffusione di «gruppi gerarchicamente strutturati con cellule semiautonome», le

---

[117] A questi comportamenti si aggiunge, a norma dello stesso art. 1, *la minaccia* di compiere attentati alla vita di una persona che possono causarne il decesso e *la minaccia* di manomettere o interrompere la fornitura di acqua, energia o altre risorse naturali fondamentali il cui effetto metta in pericolo vite umane.

quali ricorrono sempre più frequentemente all'impiego delle nuove tecnologie - in particolare a Internet - per porre in essere le loro condotte. Nel successivo Considerando n. 4, poi, emerge che i terroristi utilizzano Internet come campo d'addestramento virtuale, con l'obbiettivo di «ispirare e mobilitare reti terroristiche locali e singoli individui in Europa» e che la rete e lo spazio cibernetico costituiscono fonte di informazioni sulle risorse e sui metodi terroristici[118]. Infine, il Considerando n. 9 della stessa decisione-quadro prevede che gli Stati predispongano forme di tutela uniformi, per la prevenzione delle *nuove forme di terrorismo* ed in particolare della provocazione, del reclutamento e dell'addestramento a fini terroristici.

Orbene, dall'esame delle predette disposizioni, emerge come il legislatore europeo si sia occupato delle interazioni fra il terrorismo e le nuove tecnologie sin dalla prima definizione del fenomeno criminoso in questione. Tuttavia, dalla lettura dell'art. 1 della decisione-quadro 2002/475/GAI, sembra che il legislatore sovranazionale abbia preferito sacrificare il principio di determinatezza in favore di una definizione quanto più ampia possibile di terrorismo, attese le multiformi manifestazioni che quest'ultimo ha assunto nel corso del tempo. Ne è prova l'impiego di espressioni alquanto generiche per descrivere le possibili finalità degli atti terroristici. In particolare, le maggiori difficoltà interpretative si riscontrano con riferimento alla terza finalità, ovverosia «*destabilizzare gravemente o distruggere le strutture politiche fondamentali, costituzionali, economiche o sociali di un Paese o di un'organizzazione internazionale*». Infatti dalla lettera della norma non si evince esattamente in cosa si sostanzi detta «destabilizzazione», né tantomeno in cosa consistano le strutture politicamente fondamentali del Paese[119].

---

[118] Considerando n. 4 decisione-quadro 2008/919/GAI: «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».

[119] Sul punto potrebbe soccorrere la successiva direttiva 114/08/CE del Consiglio dell'8.3.2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, in cui viene fornita la seguente

6.2. La definizione italiana di condotte con finalità di terrorismo (art. 270-sexies c.p.)

L'art. 270-*sexies* c.p. fornisce la definizione italiana di *condotte con finalità di terrorismo,* mutuando solo parzialmente la previsione dell'art. 1 della decisione-quadro 2002/475/GAI, dedicato, come si è detto, ai *reati terroristici*. Infatti il legislatore nazionale ha scelto di riprodurre pedissequamente soltanto la prima parte della norma europea, omettendo di tipizzare le condotte terroristiche[120].

La *ratio* alla base di questa scelta definitoria sarebbe riconducibile alla necessità di adottare una definizione quanto più ampia possibile, al fine di poter sussumere entro l'art. 270-*sexies* c.p. anche tutte le nuove forme di manifestazione del terrorismo, purché dotate dei requisiti prescritti[121]. Alla medesima funzione assolve la "clausola in bianco" con cui si chiude l'art. 270-*sexies* c.p., che consente l'automatico adeguamento del nostro ordinamento rispetto alle nuove condotte definite terroristiche da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia[122].

Ad ogni buon conto si può criticamente osservare come la scelta di qualificare la natura terroristica delle condotte sulla base del solo elemento

---

definizione di infrastruttura critica: «un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni».

[120] S. CRISPINO, *Finalità di terrorismo, snodi ermeneutici e ruolo dell'interpretazione conforme. I giudici tra indeterminatezza delle fattispecie e fonti sovranazionali*, in *Dir. Pen. Cont*., 1/2017, pp. 227 e ss., in cui l'autore evidenzia che l'art. 270-*sexies* c.p., attesi i rapporti che lo legano all'art. 1 della decisione-quadro 202/475/GAI, è un esempio di *eterointegrazione parziale* del diritto penale interno mediante il diritto europeo.

[121] A. VALSECCHI, *Brevi osservazioni di diritto penale sostanziale*, in *Dir. Pen. Proc.*, 10/2005, p. 1226.

[122] Sul funzionamento della "clausola in bianco" *ex* art. 270-*sexies* c.p. si veda Cass. pen., Sez. I, sent. 11.10.2006, n. 1072, in cui i giudici affermano che: «questo rinvio – dinamico o formale – fa sì che quella dell'art. 270-*sexies* c.p. costituisca una definizione aperta, destinata, cioè, ad estendersi o a restringersi per effetto non solo delle convenzioni internazionali già ratificate, ma anche di quelle future alle quali sarà prestata adesione».

psicologico del reato e precisamente delle finalità perseguite dal soggetto agente appare poco convincente per almeno due motivi.

Per un verso, si rischia di acuire la carenza di determinatezza già segnalata in riferimento all'art. 1 della decisione-quadro 2002/475/GAI, atteso che nell'art. 270-*sexies* c.p. è stata omessa financo la tipizzazione delle condotte.

Per altro verso, la definizione italiana di condotte con finalità di terrorismo induce l'interprete meno avveduto a ritenere che la natura del fenomeno sia esclusivamente psicologica, a nulla rilevando la concreta offensività del reato. Conseguentemente si rischierebbe di sussumere entro l'art. 270-*sexies* c.p. anche quelle condotte che, ancorché poste in essere con la finalità prescritta, siano prive di qualsivoglia idoneità oggettiva in ordine alla sua realizzazione, con violazione del principio *cogitationis poenam nemo patitur*.

6.3. I presupposti oggettivi della finalità di terrorismo individuati dalla giurisprudenza di legittimità

La Corte di Cassazione, con la sentenza del 27.6.2014, n. 28009[123], ha avvertito la necessità di valorizzare il profilo oggettivo del reato terroristico, predisponendo un *sistema di criteri* che consentano, da un lato, di individuare le condotte sussumibili entro l'art. 270-*sexies* c.p. e, dall'altro lato, di espungere dall'area di applicabilità della norma le condotte che - sebbene poste in essere per perseguire una delle finalità elencate – difettino, sotto il profilo oggettivo, di idoneità offensiva[124].

---

[123] Cass. pen., Sez. VI, sent. 15 maggio 2014 (dep. 27 giugno 2014), n. 28009. Per un commento alla sentenza si rinvia M. BENDONI, *Assalto al cantiere T.a.v. di Chiomonte: non fu terrorismo*, in *Cass. pen*., n. 6, 2015, pp. 2266 e ss.; A. VALSECCHI, *Attacco «no T.a.v.» e attentato per finalità terroristiche: la Cassazione fissa le coordinate fondamentali per l'interprete*, in *Quest. giust*., 3/2014, pp. 229 e ss.; A. ZACCHIA, *Osservazioni a Cass. Pen., Sez. VI, n. 28009, 15 maggio 2014*, in *Cass. pen*., 3/2015, pp. 1115 e ss.

[124] Sul punto 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*, CEDAM, 2010, pp. 205 e ss.

Tali criteri devono essere impiegati dall'interprete nell'ambito di un giudizio prognostico, da condurre collocandosi idealmente nel momento in cui l'azione è stata posta in essere[125].

Nella sentenza i giudici rifiutano di qualificare il terrorismo come fenomeno avente natura esclusivamente psicologica, imponendo all'interprete di vagliare attentamente quanto previsto dall'art. 270-*sexies* c.p. sotto il profilo oggettivo[126]. Invero la norma presenta una serie di elementi che devono connotare il comportamento terroristico affinché esso risulti idoneo alla realizzazione dei fini tipici. La sussistenza di detti elementi, tra altro, è indispensabile se si considera che la definizione *ex* art. 270-*sexies* c.p. richiede che il soggetto agente sia animato dal *dolo specifico*. Questo, come noto, impone - per definizione - che la condotta posta in essere sia concretamente connotata dall'idoneità di realizzare l'ulteriore specifico fine perseguito, atteso che la verificazione di quest'ultimo non è necessaria per l'integrazione del reato.

Tra gli elementi che devono connotare oggettivamente la condotta terroristica, figura, in primo luogo, la possibilità di «*arrecare grave danno ad un Paese o ad un'organizzazione internazionale*». Attraverso tale previsione il legislatore ha inteso attribuire al reato terroristico natura di *pericolo concreto*, che dovrà essere accertata di volta in volta dall'interprete, attraverso il paradigma della prognosi postuma, sulla base dei criteri della «*natura*» e del «*contesto*» delle condotte.

Il concetto della *natura* si riferisce al tipo della condotta posta in essere, la quale potrà consistere nel comportamento rilevante per l'integrazione del fatto tipico di un reato sufficientemente grave, quali, ad esempio, la *strage* (art. 422), il *naufragio, sommersione o disastro aviatorio* (art, 428 c.p.), il *disastro ferroviario* (art. 430), l'*omicidio* (art. 575 c.p.), il *sequestro di persona* (art. 605 c.p.).

---

[125] L. D. CERQUA, *La nozione di terrorismo tra diritto interno, diritto internazionale e diritto comunitario*, in AA.VV., V. MANES (a cura di), *L'interpretazione conforme al diritto comunitario in materia penale*, Bononia University Press, 2007, p.120.

[126] 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 Trib. Firenze (GIP), ord. 9.1.2013, (Pezzuti), in *Dir. Pen. Cont*., 21.2.2013, pp. 3 e ss.

Il concetto di *contesto*, invece, richiede di valutare la concreta offensività della condotta rispetto alle circostanze di tipo *politico, sociale, culturale* che la connotano, le quali potrebbero riguardare direttamente i *soggetti del reato* (si pensi, ad esempio, ad una particolare carica istituzionale o politica rivestita, alla loro ideologia, alla formazione culturale ricevuta) o *fattori ambientali esterni*.

Sul punto i giudici precisano che, sotto il profilo psicologico, il soggetto agente dovrà «rappresentarsi tutti gli elementi della congerie causale che conferiscono alla sua condotta l'efficienza peculiare sanzionata» - compresi la natura ed il contesto delle condotte che, si badi, non sono mere condizioni obbiettive di punibilità, bensì elementi essenziali del fatto tipico - e volere che gli stessi influiscano «sulla serie nella quale il suo comportamento confluisce»[127].

I giudici offrono quindi un esame delle finalità che, *ex* art. 270-*sexies* c.p., devono alternativamente orientare la condotta terroristica, soffermandosi su quella consistente nel *costringere i poteri pubblici (o un'organizzazione internazionale) a compiere o astenersi dal compiere un qualsiasi atto*.

Invero il perseguimento della finalità in parola mina più autenticamente alla *Personalità dello Stato*, perché l'opera di costrizione menoma direttamente il regolare funzionamento del *metodo democratico costituzionale*, che la massima espressione del suddetto bene giuridico, siccome strumento per l'adozione delle scelte politiche che interessano tutti i consociati (inclusi coloro che non si identificano nella maggioranza parlamentare).

La Cassazione, poi, evidenzia come dalla suddetta finalità emergano dei peculiari criteri oggettivi che devono connotare la relativa condotta.

Il primo criterio consiste nella «*scala della decisione*» potenzialmente imposta al potere pubblico. In altre parole, secondo i giudici, la costrizione dei poteri pubblici a compiere o ad omettere di compiere qualcosa deve avere ad oggetto una questione particolarmente rilevante, capace - per l'implicazione che

[127] Cass. pen., Sez. VI, sent. 15.5.2014, n. 28009, p. 23.

ne deriva in punto di tenuta delle attribuzioni costituzionali - di influenzare lo svolgimento della vita associata[128].

Il secondo criterio è rappresentato dalla «*macrodimensione del fenomeno*», che deve emergere dall'«*interferenza tra la costrizione e il grave danno*»[129].

Il terzo elemento, infine, è rappresentato dalla «*illegittimità del metodo utilizzato per perseguire il fine di costrizione*»[130], che sussisterà ogniqualvolta lo Stato assuma delle scelte attraverso un metodo difforme da quello democratico costituzionalmente orientato.

In conclusione, si può osservare come la Corte escluda che la natura del terrorismo sia esclusivamente psicologica, presupponendo una condotta concretamente idonea, nel rispetto dei principi di materialità ed offensività, a realizzare i fini tipici descritti dalla norma. Invero l'*actio finium regundorum*,

---

[128] Cass. pen., Sez. VI, sent. 15.5.2014, n. 28009, p. 25, ove il collegio osserva: «se la "costrizione" è evento paragonabile al dissesto delle istituzioni od alla intimidazione della popolazione nel suo insieme, se la "costrizione" è comunque perseguita dall'agente nella consapevolezza e nella volontà di provocare il rischio di un "grave danno" per il Paese intero, allora detta "costrizione" non potrà che avere ad oggetto una decisione che incida significativamente su una scala sociale ed istituzionale corrispondente». Diversamente i giudici aggiungono che: «Non sono solo il buon senso ed il valore semantico e storico delle parole ad escludere che possa e debba parlarsi di terrorismo per qualunque pressione esercitata su un pubblico ufficiale, sia pure mediante la commissione di un reato».

[129] Cass. pen., Sez. VI, sent. 15.5.2014, n. 28009, p. 25. Il secondo criterio è connotato da un elevato grado di indeterminatezza dal momento che, da un lato, la parola «grave» ha scarsa capacità descrittiva e, dall'altro, la nozione di «danno» è opinabile quando si parla di obbiettivi politicamente rilevanti. Inoltre, poco oltre (p. 27), i giudici si premurano di precisare che: «[…] il fine di "costrizione" non può assumere dimensione terroristica per il sol fatto che la condotta strumentale contrasta con un precetto penalmente sanzionato. Si guardi alla categoria dei reati "politici" (secondo la definizione giuridicamente rilevante che discende dall'art. 8, co. 3, c.p.: non ogni atto penalmente illecito, che sia politicamente orientato in senso obiettivo o soggettivo, può integrare la nuova nozione di terrorismo».

[130] Cass. pen., Sez. VI, sent. 15.5.2014, n. 28009, p. 26, in cui il collegio afferma che: «Se ottenuta mediante comportamenti leciti, come il libero dispiegarsi del dibattito sociale e del conflitto politico, anche la più pressante influenza sul procedimento di formazione della volontà delle istituzioni pubbliche non può assumere rilevanza. Lo stesso ricorso al termine "costrizione", del resto, evoca in qualche modo l'idea di una pressione indebita e nel contempo capace (almeno nelle intenzioni dell'agente) di alterare le regole ordinarie del procedimento decisionale. Non v'è dubbio insomma che la costrizione debba essere attuata "indebitamente", anche se la norma nazionale non ha ripreso la specifica qualificazione che segna invece il suo corrispondente nella Decisione-quadro ormai più volte citata [2002/475/ GAI n.d.r.]».

volta a stabilire la sussumibilità del fatto commesso entro l'art. 270-*sexies* c.p. e quindi la sua natura terroristica, presuppone l'accertamento della sussistenza di tutti i predetti criteri oggettivi - sia quelli normativamente previsti sia quelli frutto dell'interpretazione giurisprudenziale – e, sotto il profilo soggettivo, del dolo specifico di una delle finalità tipizzate nella disposizione succitata. La più autorevole dottrina in materia si dimostra concorde con la giurisprudenza di legittimità, tanto che in proposito si è parlato di un vero e proprio *metodo terroristico*[131].

6.4. Le tecniche incriminatrici anticipatorie della soglia della punibilità impiegate nella tipizzazione dei reati terroristici

L'esame della disciplina italiana dei reati terroristici non può dirsi completa senza il riferimento alle tecniche incriminatrici impiegate per la tipizzazione delle relative fattispecie astratte.

Esse si connotano per l'*arretramento della soglia della punibilità*, attraverso l'impiego degli schemi del *reato di pericolo*, dell'*attentato*, nonché, sotto il profilo psicologico, del *dolo specifico*[132].

---

[131] V. VALENTINI, *Diritto penale intertemporale: logiche continentali ed ermeneutica europea*, Giuffrè, 2012, pp. 70 e ss., in cui l'autore spiega come la dottrina sia concorde nel ritenere che il terrorismo si connoti oggettivamente per l'impiego di un *metodo*, per contrastare il quale è necessario fare ricorso alla *law of war*. Inoltre cfr. S. CENTONZE, L. GIOVEDÌ, op. cit., pp. 198-199, in cui gli autori affermano che: «La finalità di terrorismo, intesa come circostanza aggravante, sembra essere stata prevalentemente interpretata nel senso di "metodo utilizzato": anche laddove la stessa rientra tra gli elementi costitutivi della fattispecie (artt. 270-*bis*, *quater* e *quinquies* c.p.) ne viene descritta la portata in termini prevalentemente oggettivi» ed effettuano un interessante confronto tra il *metodo terroristico* e quello *mafioso*.

[132] A. SERENI, *Delitti contro la personalità dello Stato*, in AA.VV., A. FIORELLA (a cura di), *Questioni fondamentali della parte speciale del diritto penale*, Giappichelli, 2019, pp. 543-606, in cui l'autore afferma che «i delitti contro la personalità dello Stato rievocano, nella stessa definizione formale, il clima totalitario fascista in cui vide la luce il codice Rocco. I delitti di attentato, associativi e d'opinione, i delitti contro i segreti di Stato e del tempo di guerra sono contraddistinti tutti da un sensibile anticipo della punibilità. Ancor oggi questi reati appaiono in perenne bilico tra nuove esigenze securitarie e maggior attenzione per le ragioni del garantismo penale». Inoltre, per un esame critico del rapporto sussistente fra (*ratio dei*) delitti contro la

L'anticipazione della rilevanza penale - la quale, con riferimento ai delitti previsti nel Titolo I del Libro II del codice penale, è retaggio dell'esperienza autoritaristica - viene utilizzata dal legislatore nazionale per soddisfare le prescrizioni europee in materia di prevenzione del terrorismo, che si esamineranno diffusamente nel Capitolo successivo.

Infatti, la direttiva 2017/541, solo per fare un esempio, ha imposto agli Stati di adottare le misure necessarie per assicurare la punibilità, come reati, di fatti che, privati della finalità terroristica, potrebbero risultare penalmente irrilevanti[133]. Trattasi, ad esempio, del *reclutamento a fini terroristici* (art. 6), della *fornitura* e *ricezione* di *addestramento per il compimento di attività terroristiche* (artt. 7 e 8) e dei *viaggi a fini terroristici* (art. 9). Le relative condotte, secondo la formulazione della direttiva, devono essere compiute, sotto il profilo psicologico, con il dolo specifico di commettere o contribuire alla commissione di un reato di terrorismo, la realizzazione del quale, dunque, non è necessaria per l'integrazione del reato.

Orbene, è evidente come - a tacere delle difficoltà probatorie in ordine al dolo specifico di commettere un reato terroristico - si corra il rischio di punire comportamenti, quali ad esempio i viaggi all'estero o la consultazione di siti contenenti istruzioni sul maneggiamento di esplosivi o sostanze nocive (abitualmente impiegate in determinati settori produttivi) o informazioni sull'ideologia e il metodo di gruppi terroristici (che potrebbero interessare studiosi della materia), che in mancanza della realizzazione dello scopo terroristico (non

---

Personalità dello Stato, anticipazione della rilevanza penale e diritto penale dell'emergenza, si rinvia a D. VALITUTTI, *I delitti contro la personalità dello Stato tra delitto politico e diritto penale del nemico: una ricostruzione critica*, Il Mulino, 2015, pp. 335-360.

[133] La direttiva 2017/541 del 15.3.2017, che ha sostituito la decisione quadro 2002/475/GAI, è l'ultima in materia di lotta contro il terrorismo in ordine di tempo (se si omette di considerare la direttiva (UE) 2017/853, che, più precisamente, è dedicata al controllo dell'acquisizione e della detenzione di armi). Essa ha imposto agli Stati di punire, qualificandoli come reato: la "*Pubblica provocazione per commettere reati di terrorismo*" (art. 5), il "*Reclutamento a fini terroristici*" (art. 6), la "*Fornitura di addestramento a fini terroristici*" (art. 7), la "*Ricezione di addestramento a fini terroristici*" (art. 8), il "*Viaggi a fini terroristici*" (art. 9), l'"*Organizzazione o agevolazione di viaggi a fini terroristici*" (art. 10), il "*Finanziamento del terrorismo*" (art. 11), gli "*Altri reati connessi ad attività terroristiche*" (art. 12).

richiesta per l'integrazione del reato, in ragione del dolo specifico), astrattamente resterebbero privi di qualsivoglia rilievo penale sotto il profilo oggettivo[134].

Inoltre la scarsa determinatezza delle condotte previste dalla direttiva, consente ai legislatori nazionali (vincolati solo in relazione agli obiettivi) di introdurre nei rispettivi ordinamenti fattispecie di reato che consentono di punire la mera intenzione di commettere il reato terroristico – con violazione del *principio cogitationis nemo patitur* - senza la necessità di comportamenti dotati di concreta idoneità offensiva.

I profili critici che attengono alle suddette tecniche di incriminazione volte all'anticipazione della rilevanza penale emergono con particolare evidenza in relazione alla fattispecie di "*Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico*" (art. 270-*bis* c.p.)[135].

Trattasi di reato di *mera condotta*, di *pericolo presunto* ed a *consumazione anticipata*, che, sotto il profilo psicologico, richiede il *dolo specifico* del compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico. In altri termini è lo stesso legislatore a ritenere che la *promozione*, *costituzione, organizzazione, direzione e finanziamento* di *associazioni che sol si propongono il compimento degli atti predetti* (la cui realizzazione non è necessaria ai fini dell'integrazione del reato) - senza che il giudice ne accerti

---

[134] La Proposta COM/2015/0625 final - 2015/0281 (COD), relativa alla direttiva in parola, evidenzia il rischio che possa sussumersi, entro la fattispecie di reclutamento, la navigazione in siti internet da cui poter ricavare informazioni relative al terrorismo. Sullo specifico punto si veda altresì il Considerando n. 11 della Direttiva UE/2017/541, che opera una distinzione in tema di *auto-apprendimento*. Questo, anche qualora sia posto in essere attraverso l'utilizzo della rete internet o di altro materiale didattico, potrebbe considerarsi "ricezione di addestramento" solo se risulta provato che esso deriva da una condotta attiva e che sia stato effettuato con l'intento di commettere o di contribuire a commettere un reato di terrorismo. Detta intenzione potrebbe dedursi dal tipo di materiale consultato e dalla frequenza della consultazione. Inoltre cfr. V. MASARONE, *op. cit.*, p. 20, in cui l'autrice, tra le attività astrattamente lecite rilevanti ai fini dell'integrazione del reato di ricezione di addestramento (art. 8 della direttiva 2017/541), ricomprende la frequenza di un corso di chimica all'università.

[135] N. GIORDANA, *L'art. 270-bis disciplina cardine dell'antiterrorismo. Un vestito sempre attuale che si conforma alle recenti correnti fondamentaliste di matrice islamica*, in *Giur. Pen. web*, 20.12.2014, in *https://www.giurisprudenzapenale.com/2014/12/20/art-270-bis-c-p-disciplina-cardine-dellantiterrorismo-un-vestito-sempre-attuale-che-si-conforma-alle-recenti-correnti-fondamentaliste-di-matrice-islamica/*.

l'idoneità offensiva in concerto - siano pericolose per la Personalità dello Sato e vadano pertanto punite[136].

Siffatta impostazione è sintomatica dell'origine autoritaristica della categoria dei reati contro la Personalità dello Stato – incompatibile con l'attuale ordine costituzionale - in accordo alla quale, per ritenere l'illiceità penale di un'associazione, era sufficiente che la stessa abbracciasse un'ideologia difforme da quella dello Stato-regime.

Ebbene, la tecnica di incriminazione impiegata per la costruzione della fattispecie prevista dall'art. 270-*bis* c.p. produce una doppia anticipazione punitiva. Essa, da un lato, ritiene penalmente rilevanti le condotte associative, le quali, oltre a ricevere espressa tutela costituzionale (art. 18 Cost.), si collocano in una fase ben anteriore a quella degli atti preparatori del delitto (risultando quindi irrilevanti sinanco per il tentativo). Dall'altro lato, l'art. 270-*bis* c.p. punisce le suddette condotte solo per il fine che le costituende associazioni si propongo (quindi sulla base di un requisito squisitamente psicologico), senza richiedere che esse, sotto il profilo oggettivo, presentino elementi da cui dedurne la concreta idoneità offensiva[137].

Nel complesso quadro appena descritto, emerge la necessità di individuare dei criteri che consentano di distinguere le condotte di attiva appartenenza alle

---

[136] Per un esame della fattispecie di "*Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico*" (art. 270-*bis* c.p.) e dei relativi profili critici si rinvia a M. PELISSERO, *Reati contro la personalità dello Stato e contro l'ordine pubblico*, Giappichelli, 2010, pp. 55-74 e 185-197; P. BALBO, *Il terrorismo le fattispecie di un reato in evoluzione nelle disposizioni italiane ed internazionali*, Halley, 2007, pp. 25 e ss.; R. BARTOLI, M. PELISSERO, S. SEMINARA, *Diritto penale – Lineamenti di parte speciale*, Giappichelli, 2021, pp. 785-789; V. MASARONE, *Politica criminale e diritto penale nel contrasto al terrorismo internazionale*, Ed. Scientifiche Italiane, 2013, pp. 253 e ss.

[137] M. PELISSERO, *Contrasto al terrorismo internazionale e diritto penale al limite*, in *Terr. e dir. pen*., 8/2016, pp. 99 e ss., in cui l'autore spiega che la tecnica incriminatrice secondo la quale è strutturata la fattispecie *ex* art. 270-*bis* c.p. deroga al principio *cogitationis poenam nemo patitutr* (art. 115, co. 1, c.p.). Questo, come noto, ritiene non punibile il mero accordo allo scopo di commettere un reato (quando questo non sia commesso). Sul punto, inoltre, si veda Cass., pen., Sez. I, sent. 6.10.2015, n. 47489, p. 4, con nota di S. ZIRULIA, *Apologia dell'IS via internet e arresti domiciliari. Prime prove di tenuta del sistema penale rispetto alla nuova minaccia terroristica*, in *Dir. Pen. Comp*., 14.12.2015.

associazioni terroristiche (di promozione, costituzione, organizzazione, direzione, finanziamento o mera partecipazione) - che sono penalmente rilevanti - dalla militanza in associazioni politiche che, pur presentando ideologie contrarie a quelle della maggioranza, di protesta o sinanco affini – entro certi limiti - a quelle fatte proprie dai gruppi terroristici, operino conformemente al metodo democratico[138].

Invero, nel rispetto del principio di offensività, la sussumibilità entro l'art. 270-*bis* c.p. delle condotte di promozione, costituzione, organizzazione, direzione, finanziamento di associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo presuppone che queste ultime presentino una struttura organizzativa dotata di un *grado di effettività tale da rendere quantomeno possibile l'attuazione del progetto criminoso*[139]. Detta effettività deve essere commisurata all'*idoneità della struttura* alla realizzazione di una serie - anche indeterminata - di atti di violenza con finalità di terrorismo, cioè all'attuazione del programma comune dei suoi aderenti[140].

La necessità che le condotte rilevanti *ex* art. 270-*bis* c.p. siano caratterizzate da concreta idoneità offensiva è stata sostenuta anche dalla Corte di Cassazione, secondo la quale, ai fini dell'integrazione della fattispecie di "*Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico*", non è sufficiente il mero legame tra più persone - seppur caratterizzato dalla *mala intentio* – se il *vinculum* non presenta quei

---

[138] C. CUPELLI, *Il nuovo art. 270-bis c.p.: emergenze di tutela e deficit di determinatezza?* in *Cass. pen.*, 2/2002, pp. 901 e ss.

[139] Cass. pen., Sez. I, sent., 11.10.2006, n. 1072. Il requisito dell'*organizzazione stabile* ed effettiva, tale da rendere possibile l'attuazione del programma criminale da parte dell'associazione, non implica la sussistenza di particolari schemi organizzativi tipici, essendo sufficiente che i modelli di aggregazione tra sodali integrino un *minimun* organizzativo. È per tale ragione che si ritiene che anche un'organizzazione associativa di tipo rudimentale integri il reato, purché «sia però capace di porre in essere numerosi atti di violenza contro enti ed istituzioni, idonei a condizionarne il funzionamento».

[140] Questa *effettività* e *idoneità* potrebbero ravvisarsi, ad esempio, in relazione al patrimonio di mezzi e uomini pronti al compimento di atti di terrorismo, ai caratteri strutturali dell'associazione riferiti al territorio, alle strutture materiali delle quali la stessa concretamente dispone.

caratteri di stabilità ed organizzazione minimi, tali da far presumere la concreta idoneità alla realizzazione del fine criminoso preso di mira dagli associati[141].

7. Osservazioni conclusive

L'avvento della *cibernetica*, che è la tecnologia che si occupa dell'elaborazione e della trasmissione dell'informazione fra sistemi complessi, ha rivoluzionato profondamente la socialità e i rapporti interumani. Questi oggi si possono svolgere integralmente (o almeno per parti rilevanti) nel *cyberspazio*, ovverosia un non-luogo dematerializzato, detemporalizzato e depersonalizzato non assoggettabile al paradigma tradizionale della *sovranità*.

In questo contesto sono emersi *nuovi interessi*, riconducibili alla *cybersicurezza*. Questo bene giuridico non può essere adeguatamente tutelato attraverso le *fattispecie informatiche,* introdotte dal legislatore italiano trent'anni or sono e da allora rimaste sostanzialmente immutate[142].

I reati che offendono il nuovo benne giuridico sono i *cybercrimes*. Essi sono commessi nel cyberspazio (elemento essenziale del fatto tipico) e non presuppongono, quale oggetto materiale del reato, un computer o un sistema

---

[141] Cass. pen., Sez. I, sent. 15.6.2006, n. 30824, in cui i giudici osservano che, per l'integrazione del delitto *ex* art. 270-*bis* c.p. (nonostante la struttura di pericolo presunto) è necessaria - nel rispetto del principio di offensività - «l'esistenza di una struttura organizzata, con un programma comune fra i partecipanti, finalizzato a sovvertire violentemente l'ordinamento dello Stato e accompagnato da progetti concreti e attuali di consumazione di atti di violenza»; Cass. pen., Sez. I, sent. 11.5.2000, n. 3486, in cui si legge che: «[…] la semplice idea eversiva, non accompagnata da propositi concreti e attuali di violenza, non vale a integrare il reato, ricevendo tutela proprio dall'assetto costituzionale dello Stato che essa, contraddittoriamente, mira a travolgere […]».

[142] R. BRIGHI, P. G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in Federalismi, 8.9.2021, pp. 18-42; L. PICOTTI, *Reati informatici, riservatezza, identità digitale*, op. cit., p. 17; F. B. MORELLI, *La giurisprudenza costituzionale italiana tra diritto alla riservatezza e potere di controllo sulle informazioni personali*, op. cit., p. 41; R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*, op. cit., pp. 1-2. Per la disciplina eurounitaria in materia di *cybersecurity* si veda il più recente Regolamento (UE) 2019/881 (c.d. *Cybersecurity Act*).

informatico. La commissione delle condotte dei reati cibernetici, che consistono in comportamenti rilevanti rispetto a reati già puniti dal codice penale, è animata dal dolo specifico, con finalità di volta in volta individuate dal legislatore[143].

Il *cybercrime* commesso con finalità terroristiche è il *cyberterrorismo*. Questo, diversamente dall'impostazione assunta dalla dottrina tradizionale, non può essere regolato attraverso la mera giustapposizione delle norme in materia di reati informatici (attesa la perdurante lacuna in materia di *cybercrimes* nel nostro ordinamento) e reati terroristici[144]. Invero, la scarsa giuridicità dei tentativi definitori del fenomeno impone di approfondirne la componente terroristica, per vagliare l'applicabilità della relativa disciplina (artt. 270-*bis* c.p. e ss.) *tout court* allo stesso. Ebbene, l'esame della normativa italiana in materia rivela come il cyberterrorismo presenti delle peculiarità tali da richiedere l'introduzione di un'autonoma fattispecie, che – nel rispetto dei principi di *determinatezza* ed *offensività* – tipizzi adeguatamente il reato sia sotto il profilo oggettivo che soggettivo. Con riguardo al primo aspetto sarà necessario descrivere in modo determinato le condotte del reato, con particolare attenzione per il significato che assumono gli elementi della *natura* e del *contesto* (*ex* art. 270-*sexies* c.p.) in ambito cibernetico. Per quanto attiene al profilo soggettivo (finalistico), invece, sarà necessario prevedere l'ulteriore scopo specifico che può animare i terroristi cibernetici (oltre a quelli già previsti dall'art. 270-*sexies* c.p.), ovverosia

---

[143] R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, op. cit., (in particolare il paragrafo *Il "nuovo millennio" ed il passaggio dal computer crime al cybercrime*), pp. 3-5; F. RESTA, *Virtualità del crimine. Dai reati informatici ai cybercrimes*, op.cit., pp. 102 e ss.; L. PICOTTI (a cura di), *Tutela penale della persona e nuove tecnologie*, op. cit., pp. 35 e ss.; AA.VV, C. PARODI, V. SELLAROLI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete,* Giuffrè, 2020, p. 721 e ss.; P. M. SABELLA, *Il fenomeno del cybercrime nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo,* op. cit., p. 147 e ss.

[144] F. VIGNERI, *Cyberterrorismo: realtà o finzione?*, op. cit., pp. 13; A. M. TALIHÄRM*, Cyberterrorism: in theory or in practice?*, op. cit., pp. 63-64; M. C. DE VIVO, G. RICCI, *Diritto, crimini e tecnologie*, op. cit., p. 14; P. M. SABELLA, *Il fenomeno dei cybercrimes nello spazio giuridico contemporaneo*, op. cit., pp. 139-176.

condizionare subdolamente – alterando il metodo democratico - le scelte politiche dei cittadini e di riflesso la Politica dello stato.

CAPITOLO II

La strategia multisettoriale europea per la prevenzione dei reati cibernetici e del cyberterrorismo

SOMMARIO: 1. L'alba di una normativa per la prevenzione del cyberterrorismo: l'introduzione delle prime fattispecie dei reati cibernetici (Convenzione di Budapest del 2001) e la distruzione delle infrastrutture critiche dello Stato come scopo terroristico (direttiva 2008/114/CE). – 2. La prevenzione degli attacchi terroristici contro i sistemi di informazione (direttiva 2013/40/UE). – 2.1. Le fattispecie di reato tipizzate dalla direttiva 2013/40/UE. - 2.2. I casi di non punibilità previsti dalla direttiva 2013/40/UE. – 2.3. Le circostanze aggravanti del reato di "Interferenza illecita" (art. 9 della direttiva 2013/40/UE) ed il mancato adeguamento, da parte del legislatore italiano, della risposta sanzionatoria per i corrispondenti reati. - 3. Il contrasto preventivo degli attacchi ai sistemi informativi previsto dalla direttiva (UE) 2016/1148 (NIS). - 3.1. L'ambito applicativo della direttiva NIS e le definizioni più rilevanti, in particolare quella di «incidente» (art. 4, par. 7). - 3.2. La strategia nazionale per la tutela preventiva della sicurezza della rete e dei sistemi informativi (art. 7 della direttiva NIS). - 4. Il regolamento (UE) 2019/881 (c.d. *Cybersecurity Act*): oggetto e ambito applicativo. – 4.1. La definizione europea di cybersicurezza come bene giuridico comune ai reati cibernetici (art. 2, n. 1 del *Cybersecurity Act*). - 4.2. L'evoluzione dell'Agenzia europea per la cybersicurezza (ENISA): dal regolamento (CE) 460/2004 di istituzione al regolamento (UE) 2019/881 di riforma. - 4.3. L'alfabetizzazione cibernetica come misura per la prevenzione dei reati cibernetici. - 5. La *cyberresilienza* dell'Unione europea: etimologia del termine. - 5.1. Il concetto di *resilienza* nell'attuale quadro normativo e socioculturale. - 5.2. La *resilienza* in ambito cibernetico. - 6. L'evoluzione della normativa europea in materia di lotta al terrorismo e alla radicalizzazione violenta: interazioni con la legislazione in materia di reati cibernetici. - 6.1. Il connubio fra Internet e terrorismo: le fattispecie previste dalla direttiva (UE) 2017/541 per contrastare il

fenomeno. - 6.2. Il terrorismo *online* e la strategia europea per il suo contrasto preventivo: le misure della rimozione e del blocco (art. 21 della direttiva 2017/541). - 6.3. Il regolamento (UE) 2021/784 per il contrasto della diffusione dei contenuti terroristici *online* e dell'uso dei servizi di *hosting* a fini terroristici. – 7. Osservazioni conclusive.

1. L'alba di una normativa per la prevenzione del cyberterrorismo: l'introduzione delle prime fattispecie dei reati cibernetici (Convenzione di Budapest del 2001) e la distruzione delle infrastrutture critiche dello Stato come scopo terroristico (direttiva 2008/114/CE)

Il legislatore europeo ha dimostrato interesse per la *fase cibernetica della rivoluzione informatica* sin dagli albori del terzo millennio.

In data 23 novembre 2001, il Consiglio d'Europa ha approvato il primo strumento normativo internazionale disciplinante in modo sistematico la materia dei *cybercrimes*. Trattasi della Convenzione di Budapest[145], nella quale è stata riconosciuta l'accresciuta potenzialità criminogena della *cibernetica* (ed in particolare del *cyberspace*) rispetto all'*informatica*[146]. Invero gli Stati firmatari hanno ritenuto opportuno avviare una cooperazione internazionale in materia penale, al fine di *prevenire* tutte le condotte che offendono nuovi beni quali la *segretezza*, l'*integrità* e la *disponibilità* di *sistemi informatici*, *reti*, *informazioni* e

---

[145] *Convention on Cybercrime*, *Council of Europe*, Budapest, 23.11.2001.

[146] Nel Preambolo alla Convenzione di Budapest, gli Stati dichiarano di essere: «[…] convinti della necessità di perseguire, come questione prioritaria, una politica comune in campo penale, finalizzata alla protezione della società contro la criminalità informatica, adottando una legislazione appropriata e sviluppando la cooperazione internazionale; consci dei profondi cambiamenti dipendenti dall'introduzione della tecnologia digitale, dalla convergenza e costante globalizzazione delle reti informatiche; preoccupati dei rischi che le reti informatiche e le informazioni in formato elettronico possano anche essere utilizzate per commettere reati e che le prove connesse a tali reati possano essere conservate e trasferite tramite queste reti; riconoscendo la necessità della cooperazione tra gli Stati e le società private nella lotta alla criminalità informatica e la necessità di tutelare gli interessi legittimi nell'uso e nello sviluppo delle tecnologie informatiche […]».

dati informatici[147]. La Convenzione in parola, inoltre, prevede la tipizzazione di ben sette fattispecie di reato, oltre all'incriminazione delle condotte di pornografia infantile e quelle contro la proprietà intellettuale[148].

Procedendo secondo un ordine cronologico, il secondo atto normativo, rilevante ai fini della ricostruzione della disciplina europea in materia di reati cibernetici ed in particolare di cyberterrorismo, è rappresentato dalla direttiva 2008/114/CE dell'8 dicembre 2008, relativa all'individuazione ed alla designazione delle cosiddette *infrastrutture critiche europee* ed alla loro protezione dai reati di terrorismo[149].

---

[147] Sempre nel Preambolo alla Convenzione di Budapest vengono espressamente elencati i *nuovi beni giuridici* che gli Stati membri si prefiggono di tutelare attraverso l'introduzione delle nuove fattispecie delittuose: «[…] convinti che la presente Convenzione sia necessaria come deterrente per azioni dirette contro la segretezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dei dati informatici, così come per l'uso improprio di questi sistemi, reti ed informazioni […]». Invero l'elencazione dei predetti beni rileva sotto un duplice profilo. Da un lato, emerge come a livello sovranazionale si percepisca la necessità di tutelare penalmente interessi completamente nuovi, che hanno ormai maturato una propria identità ed autonomia, in ragione dello sviluppo registrato in ambito cibernetico. Dall'altro lato, invece, i nuovi beni giuridici partecipano della definizione del concetto di reato cibernetico, dal momento che si distinguono nettamente, ricomprendendoli, dai beni offesi dai reati informatici. Questi ultimi, come detto, si rivolgono ad offendere limitatamente l'integrità dei *computers* o, al più, dei sistemi informatici, disinteressandosi di reti, dati (che se usati impropriamente possono divenire, a loro volta, strumenti d'offesa), nonché della loro segretezza.

[148] Nella Convenzione di Budapest sono previste le seguenti fattispecie criminose: "*Accesso illegale ad un sistema informatico"* (art. 2), "*Intercettazione abusiva*" (art. 3), "*Attentato all'integrità dei dati*" (art. 4), "*Attentato all'integrità di un sistema*" (art. 5), "*Abuso di apparecchiature*" (art. 6), "*Falsificazione informatica*" (art. 7), "*Frode informatica*" (art. 8), "*Reati relativi alla pornografia infantile*" (art. 9) e "*Reati contro la proprietà intellettuale e diritti collegati*" (art. 10). Per un esame dell'esecuzione della Convenzione di Budapest nell'ordinamento italiano si consiglia la lettura di L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, in *Dir. Pen. e Proc.*, 6/2008, pp. 696 e ss.

[149] Al fine di comprendere la *ratio* che ha animato il legislatore eurounitario nell'emanare la direttiva 2008/114/CE si legga il relativo Considerando n. 1, in cui emerge che, a fronte della richiesta del Consiglio europeo di preparare una strategia globale per la protezione delle infrastrutture critiche (giugno 2004), la Commissione (in data 20.10.2004) ha adottato una comunicazione relativa alla protezione delle infrastrutture critiche nella lotta contro il terrorismo, nella quale ha indicato delle proposte per incrementare la *prevenzione, la preparazione e la risposta a livello europeo in caso di attentati terroristici che coinvolgono le infrastrutture critiche*. Sull'importanza rivestita dalle infrastrutture critiche, che ha reso necessaria un'apposita disciplina a livello europeo, si veda L. LUPARIA, *Sistema penale e criminalità Informatica*, Giuffrè, 2009, p. 45, in particolare la nota 47, in cui l'autore evidenzia che l'ambito e la tutela (anche

La direttiva, pur non essendo direttamente coinvolta nella tutela della *cybersecurity*, rappresenta uno strumento fondamentale per il contrasto dei reati terroristici e peculiarmente di quelli posti in essere ai danni delle *infrastrutture critiche dello Stato*[150]. Quest'ultimo concetto, proprio a partire dal 2008, assume centralità nelle fonti eurounitarie che disciplinano la materia dei *cybercrimes*[151]. In particolare nell'art. 2 della direttiva, vengono definiti i concetti di «infrastruttura critica» e di «infrastruttura critica europea».

Il primo concetto si riferisce ad ogni elemento o sistema (o anche parte di questo) ubicati in uno Stato membro, che risultino essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere

---

informatica) delle infrastrutture critiche sono in via di trasformazione, tanto da poter prevedere che nel giro di pochi anni esse assumeranno importanza primaria e fondamentale per la collettività». Sul punto pare opportuno osservare che l'importanza strategica delle infrastrutture critiche, e quindi delle misure per la loro tutela, è stata recentemente confermata, su piano domestico, dalla destinazione, nel Piano Nazionale di Ripresa e Resilienza (PNRR) del 13.7.2021, di una quota pari al 27% delle risorse totali alla materia della cosiddetta «transizione digitale», prevedendo altresì la creazione del *Polo Strategico Nazionale* (PSN), per la gestione in *cloud* di dati e applicazioni della Pubblica Amministrazione.

[150] Con riguardo agli attacchi cyberterroristici ai danni delle infrastrutture critiche dello Stato, A. LAVORGNA, *Cybercrimes*, RED GLOBE Press, 2020, p. 170, in cui l'autrice evidenzia che «Though still relatively rare, these types of attacks, unfortunately, are already a fact» e riporta alcuni esempi: «[…] an employee's laptop was used as an entry point to install a malware capable of affecting the operations in a water treatment plant in the USA in 2006; in late 2015, a DoS (n.d.r. *i.e*. denial of service) attack trigged a power outage in a power plant and multiple substations in Ukraine; in late 2016, a DoS attack disrupted the heating system of several houses in Finland for more than a week». Inoltre Lavorgna evidenzia che solo un numero limitato di *cyberattacks* terroristici sono stati pubblicamente attribuiti ad uno Stato nazionale e che il numero di attacchi presumibilmente riconducibili a "procuratori degli Stati" («procurators of States») - ovverosia attori non statali che vengono impiegati dagli Stati per compiere attacchi – è molto superiore (tra i casi più celebri figura quello denominato "*Stuxnet*"). Nello stesso senso S. C. MCQUADE, *Encyclopedia of Cybercrimes*, Greenwood Press, 2009, p. 55 e J. I. ROSS, *Cybercrimes*, Chelsea House, 2010, pp. 51-52. Infine cfr. R. T. UDA, *Cybercrime, Cyberterrorism, and Cyberwarfare*, Xilibris, 2009, pp. 136-137, in cui l'autore evidenzia che «Indeed, it is the job of cyber security managers to anticipate the moves of their opponent even if the anticipated attack is never realized», confermando come l'essenza della *cybersecurity* risieda nella prevenzione.

[151] Sul punto è necessario precisare che se, da un lato, come si è detto, è vero che la direttiva non è direttamente coinvolta nella tutela della *cybersecurity*, dall'altro lato, nel relativo Considerando n. 5, emerge come essa costituisca il primo passo di un graduale approccio verso l'individuazione delle infrastrutture critiche europee e la predisposizione della disciplina per la loro protezione.

economico e sociale dei cittadini[152], con la conseguenza che il danneggiamento (o, peggio, la distruzione) degli stessi produrrebbe un grave danno allo Stato.

Il tratto distintivo del secondo concetto, invece, è legato alla portata del danneggiamento (o della distruzione), il quale deve impattare, in modo significativo, sui settori essenziali – anche eterogenei - di *almeno due Stati membri*[153].

Invero, attesa la grande varietà di funzioni da erogare, la direttiva non propone un elenco tassativo di infrastrutture, bensì un metodo per la loro individuazione. Infatti, nel relativo art. 3, par. 2, si precisa che i criteri che gli Stati membri (con l'eventuale collaborazione della Commissione) devono valutare in concreto per procedere all'individuazione delle suddette infrastrutture sono: il *numero di vittime* che potenzialmente potrebbero derivare dall'atto alla

---

[152] R. T. UDA, *Cybercrime, Cyberterrorism, and Cyberwarfare*, op. cit., p. 76, in cui l'autore precisa che le *infrastrutture critiche dello Stato*, che sono sia fisiche che virtuali, consistono nel «framework around which we live our daily lives, conduct business, and function as a society, we deem these sectors as critical to our country's existence».

[153] Per una distinzione tra «infrastruttura critica» e «infrastruttura critica europea» si veda C. SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, Giuffrè, 2010, pp. 1102 e ss. e A. SPAGNOLO, S. SALUZZO (a cura di), *La responsabilità degli Stati e delle organizzazioni internazionali: nuove fattispecie, problemi di attribuzione e di accertamento*, op. cit., p. 361. Per una visione comparatistica del rapporto fra infrastruttura critica dello Stato e *cyberattack*, invece, J. E. CARTWRIGHT, *Memorandum for chiefs of the military services commanders of the combatant commands directors of the joint staff directorates*, on *Joint Terminology for Cyberspace Operations*, USDOD, 2011, p. 5, par. 10, in cui l'autore, nel fornire la definizione di «*cyberattack*», evidenzia come il concetto di infrastruttura critica sia un elemento essenziale della stessa: «A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves-for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery». In tal senso la dottrina statunitense dimostra una maggior elasticità nell'individuare collegamenti interdisciplinari fra i *cybercrimes* (in particolare il *cyberattack* nella definizione succitata) e le infrastrutture critiche, i quali nella legislazione eurounitaria, invece, restano disciplinati da atti ben distinti. Infine, per un'interessante esame delle interazioni sussistenti fra disciplina delle infrastrutture critiche e banche dati, si consigli la lettura di C. SARZANA DI S. IPPOLITO, *L'accesso illecito alle banche dati ed ai sistemi informatici pubblici*, in *Dir. Inf.*, 2007, pp. 277 e ss.

infrastruttura; le *conseguenze economiche* da valutare in termini di entità delle perdite economiche e/o del deterioramento di prodotti o servizi (comprese le potenziali conseguenze ambientali); le *conseguenze per i cittadini*, da valutare in termini di impatto sulla *fiducia*; le *sofferenze fisiche e la perturbazione della vita quotidiana*, compresa la perdita di servizi essenziali.

Alla luce di queste considerazioni risulta evidente come anche il settore delle telecomunicazioni e più in generale quello di tutti i sistemi informatici e telematici impiegati dagli organi dello Stato per assicurare dei servizi essenziali ai cittadini (non da ultimo quelli che prevedono la raccolta ed il trattamento, a vario titolo, di dati personali sensibili per scopi sanitari o di giustizia) ben possano rientrare nella definizione di *infrastruttura critica dello Stato*.

Sulla scorta di tali rilievi, non pare dunque azzardato ritenere che lo stesso *cyberspace*, inteso come luogo virtuale in cui avviene lo scambio di informazioni - non limitabile entro i ristretti confini del domicilio[154] - possa essere inteso come un'infrastruttura critica dello Stato (art. 2, lett. a, della direttiva 2008/114/CE), che quest'ultimo è chiamato a tutelare rispetto a condotte con finalità di terrorismo[155].

---

[154] Sulla non riconducibilità dei nuovi interessi giuridici al domicilio (informatico) si veda R. BORRUSO, *La tutela del documento e dei dati*, in R. BORRUSO, G. BUONOMO, G. CORASANITI, G. D'AIETTI (a cura di), *Profili penali dell'informatica*, Giuffrè, 1994, p. 28 e ss.

[155] Per un esame delle relazioni intercorrenti fra il *cyberspace* e le infrastrutture critiche si consiglia la lettura di L. MARTINO, *La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica*, CSSII UNFI, 2012, pp. 3 e ss. e S. ROBERTO, *La protezione delle Infrastrutture Critiche informatizzate*, in *Automazione e Strumentazione*, 8/2003, p. 27, in cui l'autore evidenzia che: «Il *cyberspace* sta assumendo il ruolo di *Global Information Infrastructure* ed è condiviso dalla maggior parte delle infrastrutture tecnologiche. A sua volta, l'esistenza del *cyberspace* è legata al corretto funzionamento di alcune di queste infrastrutture (rete elettrica, reti di telecomunicazioni ecc.) e che rappresentano il basamento su cui esso si poggia». Inoltre, cfr. M. PASTORELLO, *How cyberspace is used by terrorist organization: possible threats to critical infrastructures? The most recent activities of cyber counterterrorism*, in *Sicurezza, terrorismo e società*, 2/2015, p. 117, in cui emerge come, proprio in ragione del rapporto sussistente fra infrastrutture critiche e *cyberspace*, oggi non si possa più parlare di infrastrutture meramente fisiche, bensì di «*Infrastrutture Critiche Informatizzate*» (ICI). Infine, cfr. A. LAVORGNA, *Cybercrimes*, op. cit., pp. 178-179, in cui l'autrice evidenzia che il *cyberspace* non è il "miglior obbiettivo" per i cyberterroristi: «Given that terrorists – according to the utility principle - want to maximise their rewards while minimising their efforts, cyberspace could make many targets extremely difficult targets to access». Sul punto basti infatti pensare che molti *cyberattcks* presuppongono livelli assai elevati di conoscenze ed

Tra le definizioni rilevanti contenute nell'art. 2 della direttiva in esame figura anche quella di «informazioni sensibili relative alla protezione delle infrastrutture critiche». Dette informazioni, che il legislatore europeo si prefigge di tutelare, consistono in tutti quei fatti che, se divulgati, potrebbero essere usati per pianificare ed eseguire azioni tali da comportare il danneggiamento o la distruzione delle infrastrutture critiche[156]. È dunque evidente come la pianificazione e l'esecuzione delle azioni in parola potrebbero essere operate da cyberterroristi, al fine di danneggiare le infrastrutture di riferimento (art. 2, lett. d). Sul punto giova precisare che l'art. 9 della direttiva in esame prescrive che il personale addetto al trattamento delle *informazioni sensibili*, per conto di uno Stato membro o della Commissione – che deve essere oggetto di un'appropriata indagine di sicurezza - è tenuto a garantire che le stesse non vengano usate per scopi diversi dalla protezione delle infrastrutture critiche.

Ebbene, sulla scorta delle summenzionate definizioni, è dunque possibile ritenere che le infrastrutture critiche dello Stato si connotino sotto il profilo teleologico, dal momento che consistono in tutti quei settori finalizzati a garantire l'esercizio delle diverse funzioni essenziali dello Stato, delle quali beneficiano anzitutto i cittadini. Pertanto, attesa l'importanza delle infrastrutture in parola, la loro distruzione può certamente rientrare fra gli scopi terroristici astrattamente tipizzati dall'art. 1 della decisione-quadro 2002/475/GAI e, quindi, dall'art. 270-*sexies* c.p.

---

abilità in ambito informatico e cibernetico, normalmente non richieste per il compimento dei tradizionali attacchi terroristici alla portata di qualunque lupo solitario.

[156] Al fine di comprendere il livello di interazione che lega il cyberterrorismo al concetto di infrastrutture critiche dello Stato è opportuno fare riferimento a S. C. MCQUADE, *Encyclopedia of Cybercrimes,* op. cit., p. 55, in cui l'autore evidenzia che il primo ha come obbiettivo precipuo la realizzazione di attacchi ai danni delle seconde e che «the goal of so called cyberterrorism is to attack information systems to instill fear in those who have the capability to make political changes demmed necessary by the attackers». Nello stesso senso R. T. UDA, *Cybercrime, Cyberterrorism, and Cyberwarfare*, op. cit., pp. 8-9.

2. La prevenzione degli attacchi terroristici contro i sistemi di informazione (direttiva 2013/40/UE)

Nell'esame delle fonti che regolano la materia dei *cybercrimes* e che - mancante una normativa specificamente dedicata – contribuiscono alla formazione della disciplina del cyberterrorismo, non può essere tralasciata la direttiva 2013/40/UE, dedicata alla prevenzione e repressione degli attacchi posti in essere contro i sistemi di informazione (dunque non solo informatici), da parte di persone fisiche o giuridiche e, in particolare, da parte delle organizzazioni terroristiche[157].

Preliminarmente rileva osservare che il legislatore europeo, come già poteva desumersi dalla direttiva 2008/114/CE, ricomprende i sistemi di informazione entro il novero delle infrastrutture critiche. Infatti essi, da un lato, svolgono un ruolo essenziale per il mantenimento delle *funzioni vitali della società* (potendo essere impiegati in diversi settori, quali salute, sicurezza, giustizia e benessere - economico e sociale - dei cittadini) e, dall'altro lato, è indubbio che il loro danneggiamento (o distruzione) comporti un impatto significativo sullo Stato, tale da impedire che siano garantite le predette funzioni. L'importanza dei sistemi di informazione come infrastrutture critiche è confermata, tra l'altro, dal fatto che, sempre più frequentemente, essi vengono presi di mira da attacchi terroristici e, più in generale, aventi natura politica[158]. Invero i sistemi in parola oggi rivestono il ruolo di elemento chiave dell'interazione politica, sociale ed economica nell'Unione, dai quali la società, come si è detto, è ormai sempre più dipendente.

---

[157] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione, ha sostituito la decisione quadro 2005/222/GAI del Consiglio del 24 febbraio 2005.

[158] Sul punto si veda il Considerando n. 3 della direttiva 2013/40/UE, in cui si evidenzia come il numero degli attacchi terroristici ai sistemi di informazione, facenti parte dell'infrastruttura critica degli Stati membri e dell'Unione, sia in costante aumento. Il fenomeno costituisce una minaccia per la creazione di una società dell'informazione più sicura e di uno spazio di libertà, sicurezza e giustizia a livello europeo.

Proprio per questa ragione il legislatore eurounitario ha ritenuto indispensabile ravvicinare il diritto penale degli Stati membri - stabilendo norme minime relative alla definizione dei reati e delle sanzioni rilevanti - e migliorare così la cooperazione fra le autorità competenti, sia nazionali (in particolare le polizie dei diversi Stati membri) sia sovranazionali (in particolare le competenti Agenzie e gli organismi specializzati dell'Unione[159]).

Dall'esame della direttiva in parola emerge come la garanzia di un adeguato livello di protezione dei sistemi d'informazione rappresenti una delle più efficaci misure di prevenzione contro la criminalità informatica, che ha saputo sfruttare le potenzialità delle nuove tecnologie[160]. Invero la direttiva 2013/40/UE segna uno spartiacque tra il passato ed il presente della strategia europea in materia di *cybersecurity*, dal momento che, con essa, il legislatore eurounitario ha

---

[159] Tra le Agenzie che rivestono un ruolo significativo in materia si ricordano *Eurojust*, *Europol* (ed il suo Centro europeo per la criminalità informatica) e l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), della quale si dirà nel prosieguo. La bontà della strategia europea per il contrasto del cyberterrorismo è confermata dall'adozione, da parte del legislatore statunitense, di un approccio preventivo in materia. Sul punto R. T. UDA, *Cybercrime, Cyberterrorism, and Cyberwarfare*, op. cit., 57 e in J. I. ROSS, *Cybercrimes*, op. cit., p. 99, in cui l'autore chiarisce che i controlli e la protezione dai *cybercrimes* «may not lead to the elimination of cybercrime, but they will help diminish its proliferation or reduce having individuals or business victimized».

[160] E. R. LEUKFELDT, J. H. THOMAS, *The Human Factor of Cybercrime*, Routledge, 2020, pp. 305-306, in cui gli autori chiariscono che: «The late British Prime Minister Margaret Thatcher famously described publicity as the oxygen of terrorism. This pronouncement continues to resonate because although it is never their ultimate objective, publicity is what sustains effective terrorist campaigns. It follows from this that violent extremists and terrorists should take every opportunity to get their message out to as large an audience as possible by amplifying their violence via media». Nello stesso senso A. P. SCHMID, J. DE GRAAF, *Violence as communication: Insurgent terrorism and the western news media*, SAGE Publications, 1982, p. 9, in cui gli autori affermano che senza comunicazione non può esserci terrorismo. Inoltre cfr. V. NARDI, *La punibilità dell'istigazione nel contrasto al terrorismo internazionale*, in *Dir. Pen. Comp*., 1/2017, p. 120, in cui l'autrice, con particolare riferimento all'abilità dimostrata dai gruppi terroristici di sfruttare le nuove tecnologie cibernetiche afferma che: «[…] non può non considerarsi che oggigiorno la capacità diffusiva del radicalismo islamico, e dunque del terrorismo, ha trovato un supporto nelle nuove tecnologie, in particolare Internet e i *social media*. Come è emerso da alcuni studi realizzati a livello internazionale, i gruppi terroristici sono ormai divenuti particolarmente abili nello sfruttare il *web* per reclutare nuovi seguaci, trovare finanziamenti, portare avanti azioni di propaganda e sensibilizzazione e, soprattutto, per raccogliere e diffondere informazioni».

manifestato espressamente la preferenza per il contrasto preventivo (anziché repressivo) del terrorismo moderno[161]. Ciononostante, è bene precisarlo, il *quadro giuridico di riferimento per la lotta contro la criminalità informatica*, compresi gli attacchi contro i sistemi di informazione, resta imprescindibilmente quello descritto dalla *Convenzione di Budapest del 2001*[162].

Ad ogni modo il ravvicinamento del diritto penale degli Stati membri, prospettato nella direttiva in esame, appare indispensabile anche a fronte delle notevoli differenze, tuttora esistenti in materia di *cybercrimes* e *cyberterrroism*, tra i diversi ordinamenti nazionali. Infatti, come già evidenziato nel Capitolo precedente, alcuni Paesi dimostrano una maggior attenzione per il problema mentre altri, come quello italiano, continuano ad ignorare che, grazie al *cyberspace*, i terroristi possono colpire - attraverso nuove condotte dotate di maggiore pervasività - beni giuridici nuovi ed autonomi rispetto al mero domicilio (i quali, come si è detto, trovano la loro sintesi nella *cybersecurity,* v. §. 4.3. del Capitolo I)[163].

---

[161] Sul punto si veda il Considerando n. 2 della direttiva 2013/40/UE, in cui viene fatto espresso riferimento alla necessità di adottare un sistema di misure di prevenzione, come imprescindibile completamento delle forme tradizionali di risposta alla criminalità informatica nell'ambito del diritto penale.

[162] Sul punto, se è vero che, da un lato, il Considerando n. 15 della direttiva 2013/40/UE riconosce la necessità che le Istituzioni europee provvedano ad elaborare una nuova strategia - di concerto con gli Stati membri e la Commissione - dall'altro lato, lo stesso prevede anche che tale strategia muova imprescindibilmente dai principi già fissati dalla Convenzione di Budapest del 2001, la quale resta il *quadro giuridico di riferimento* per la lotta contro la criminalità informatica (compresi gli attacchi contro i sistemi di informazione) e per la stessa direttiva del 2013/40/UE.

[163] Con riguardo alla consapevolezza, maturata a livello eurounitario, circa i diversi livelli di tutela raggiunti nei singoli ordinamenti nazionali si veda il Considerando n. 27, in cui si evidenzia che il rafforzamento della cooperazione internazionale relativamente alla sicurezza dei sistemi di informazione, delle reti informatiche e dei dati informatici si rende necessario in ragione delle rilevanti lacune e delle notevoli differenze nel diritto penale sostanziale e nelle procedure penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione. Invero la carenza di uniformità può ostacolare la lotta contro la criminalità organizzata e il terrorismo, nonché complicare l'efficace cooperazione di polizia e giudiziaria in questo settore. Il ravvicinamento del diritto penale in questo settore è indispensabile a causa della dimensione transfrontaliera degli attacchi contro i moderni sistemi di informazione. Con riguardo alla consapevolezza, maturata a livello eurounitario (non anche italiano), circa la maggiore pervasività che le condotte terroristiche poste in essere nel *cyberspace* possono raggiungere, invece, il Considerando n. 16 della direttiva 2013/40/UE tiene conto delle: «[…] varie modalità con cui

In particolare la direttiva si sofferma nell'indagare l'*atteggiamento psicologico* che deve animare il soggetto agente nel porre in essere l'attacco ai sistemi di informazione. L'autore della condotta criminosa deve agire con dolo nella forma dell'«*intenzione diretta*», che, alla luce del nostro ordinamento, parrebbe doversi intendere nel senso del *dolo intenzionale*[164]. Conseguentemente, per la direttiva, sarà punibile esclusivamente colui che pone in essere un attacco ai danni di un sistema di informazione laddove persegua, come scopo finale della sua condotta, proprio l'evento descritto dalla fattispecie di riferimento.

Passando ora ad esaminare l'articolato dell'atto normativo, nell'art. 1 emerge con chiarezza che il legislatore, attraverso la direttiva, ha inteso perseguire precipuamente *tre obbiettivi*. Essi consistono, *in primis*, nello stabilire norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi di informazione; *in secundis*, nel facilitare la prevenzione di tali reati; *in tertiis*, nel migliorare la cooperazione tra autorità giudiziarie e altre autorità competenti, anche private.

Con riguardo a quest'ultimo obbiettivo, sembra che il legislatore ritenga imprescindibile, al fine di *prevenire* gli attacchi contro i sistemi di informazione, l'instaurazione di un dialogo fondato su un costante scambio di informazioni tra soggetti privati (aziende produttrici di *software* e *devices* informatici e cibernetici, nonché *service providers* e relativi *stakeholders*), autorità pubbliche e società civile[165]. Tale cooperazione dovrebbe prevalere sugli interessi individuali che – legittimamente - animano l'operato dei privati, al fine di tutelare i *sistemi di informazione*, i quali sono infrastrutture critiche dello *Stato*.

---

possono essere effettuati gli attacchi e della rapida evoluzione degli *hardware* e dei *software*», che possono essere utilizzati per commettere i nuovi *cybercrimes*.

[164] Considerando n. 16: «[…] Data la necessità di evitare una criminalizzazione di tali strumenti, quando essi siano prodotti e commercializzati per fini legittimi, come la verifica dell'affidabilità dei prodotti di tecnologia dell'informazione o la sicurezza dei sistemi di informazione, oltre al requisito dell'intenzione generale, deve essere soddisfatto anche il requisito dell'intenzione diretta di utilizzare tali strumenti per commettere uno o più reati previsti nella presente direttiva».

[165] La cooperazione, a norma del Considerando n. 23 della direttiva in esame - deve in ogni caso svolgersi nel pieno rispetto del principio dello Stato di diritto.

Secondo le previsioni della direttiva, la cooperazione deve includere la conservazione, da parte dei *fornitori di servizi*, di tutti gli elementi idonei a costituire prove in ordine all'identificazione degli autori dei reati (specie impiegando tecnologie che facciano ricorso a dati biometrici)[166]. I dati raccolti dai fornitori di servizi, che riguardino i reati tipizzati dalla direttiva, dovrebbero essere quindi messi a disposizione delle Agenzie e degli organismi specializzati dell'Unione, al fine di consentire la formazione di un quadro più completo del problema della criminalità informatica e degli attacchi alle reti ed ai sistemi dell'informazione. In questo modo si contribuirebbe alla predisposizione di una risposta più efficace contro il fenomeno, anche in chiave penale[167].

La direttiva 2013/40/UE, inoltre, prevede la definizione di alcuni rilevanti concetti, tra i quali figura quello di «*sistema di informazione*». Questo, a norma dell'art. 2, lett. a), consiste in un'apparecchiatura o in un gruppo di apparecchiature interconnesse o collegate, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma, nonché i dati informatici immagazzinati da tale apparecchiatura o gruppo di apparecchiature, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione[168].

Il *sistema di informazione*, dunque, presenta due componenti: la prima corrisponde all'*hardware* e più in generale ai *devices* impiegati per il trattamento

---

[166] Considerando n. 23 della direttiva.

[167] Il Considerando n. 24 della direttiva, con peculiare riferimento al ruolo che la cooperazione e lo scambio di informazioni possono rivestire in relazione alla prevenzione degli attacchi ai sistemi di informazione, prevede che gli Stati membri trasmettano informazioni sul *modus operandi* degli autori dei reati a Europol, ai fini dell'effettuazione di valutazioni delle minacce e di analisi strategiche in merito alla criminalità informatica.

[168] Per completezza si segnala che l'art. 2 della direttiva prevede altresì la definizione di: «*dati informatici*» (art. 2, lett. b), i quali consistono nella rappresentazione di fatti, informazioni o concetti in una forma che può essere trattata in un sistema di informazione; «*persona giuridica*» (art. 2, lett. c), consistente in un'entità che ha lo status di persona giuridica in forza del diritto applicabile (tuttavia la definizione non include gli Stati o gli organismi pubblici che agiscono nell'esercizio dell'autorità statale o le organizzazioni pubbliche internazionali); nonché di «*senza diritto*» (art. 2, lett. d), che si riferisce a quelle condotte - inclusi l'accesso, l'interferenza o l'intercettazione - non autorizzate da parte del proprietario o da un altro titolare di diritti sul sistema o su una sua parte, ovvero non consentiti a norma del diritto nazionale.

dei dati; la seconda, invece, consiste nei *dati* stessi, che sono parte integrante del sistema. Alla luce di tali rilievi, pare potersi ravvisare un rapporto analogico fra il *sistema di informazione* e la struttura tripartita del *cyberspace*, con l'effetto di estendere a quest'ultimo le tutele previste per il primo. Infatti secondo Even e Siman-Tov, come si ricorderà, lo spazio cibernetico presenta - oltre allo *human layer* - la componente del *physical layer* (corrispondente ai *devices* per il trattamento di dati) e quella del *logical layer* (corrispondente ai dati trattati).

2.1. Le fattispecie di reato tipizzate dalla direttiva 2013/40/UE

La direttiva 2013/40/UE, dopo la parte dedicata alle definizioni, prescrive che gli Stati introducano nei rispettivi ordinamenti alcuni nuovi reati, descrivendo alquanto dettagliatamente le relative fattispecie (artt. 3, 4, 5, 6 e 8).

L'art. 3 prevede l'"*Accesso illecito a sistemi di informazione*".

Sotto il *profilo oggettivo*, la condotta necessaria per integrare il reato in parola consiste nell'accesso ad un sistema di informazione (o anche solo ad una sua parte) «*senza diritto*» e «*in violazione di una misura di sicurezza*», discostandosi, con la seconda previsione, dal dettato della Convenzione di Budapest. Infatti questa, per la punibilità dei *cybercrimes*, non presuppone la violazione delle misure di sicurezza.

Con riguardo al primo connotato che deve avere l'accesso *nulla quaestio*. L'*assenza di diritto* viene definita come la mancanza di autorizzazione da parte del proprietario o del titolare di diritti sul sistema (o su una sua parte) o comunque come la contrarietà alle norme del diritto nazionale (art. 2, lett. d)[169].

Per quanto attiene al secondo connotato, invece, l'accesso abusivo andrebbe punito sol quando effettuato in violazione di una misura di sicurezza, introducendo, in tal modo, una vera e propria condizione di punibilità[170]. In

[169] Per la definizione di «senza diritto» si veda la nota precedente.

[170] La condizione in parola ha l'effetto di limitare la punibilità alle condotte più ostinate e aggressive, che siano concretamente idonee a vincere la resistenza delle misure appositamente

particolare, il concetto di misura di sicurezza rilevante ai sensi della direttiva consiste, come chiarito dalla giurisprudenza e dalla dottrina domestiche, in qualsiasi misura di protezione, anche molto bassa (come, ad esempio, una comune *password*), volta ad escludere la pubblicità del sistema. Conseguentemente il reato in esame si perfeziona ogniqualvolta vengano violate le condizioni e i limiti delle prescrizioni impartite dal titolare del sistema, indipendentemente dagli scopi specifici e dalle finalità perseguite dall'autore della condotta[171].

Tuttavia è bene segnalare che le eventuali limitazioni previste a livello eurounitario - come in questo caso la violazione delle misure di sicurezza - non possono impedire l'adozione, da parte degli Stati membri in sede di attuazione della direttiva, di *standards* più elevati per la protezione dei sistemi informatici. A livello nazionale potrebbe quindi ritenersi abusivo sinanco l'accesso che non violi misure di sicurezza. Ciononostante, il legislatore domestico che ha accolto lo *standard* di protezione minimo imposto dalla direttiva, senza innalzare oltre il livello di sicurezza per i sistemi di informazione[172].

Sempre con riguardo al perfezionamento del reato, bisogna poi evidenziare che, secondo la lettera dell'art. 3 della direttiva in esame, rileva esclusivamente la

---

predisposte. Per un'approfondita esegesi della fattispecie italiana di "*Accesso illecito ad un sistema di informazione*", con particolare attenzione per la suddetta condizione di punibilità, si rinvia a R. BARTOLI, *L'accesso abusivo a un sistema informatico (art. 615-ter c.p.) a un bivio ermeneutico teleologicamente orientato*, in *Dir. Pen. Cont*., 1/2012, p. 123 ed a R. FLOR, *Verso una rivalutazione dell'art. 615 ter c.p.?*, in *Dir. Pen. Cont.*, 2/2012, p. 126.

[171] Sul tema si veda Cass. SS.UU., sent. 27 ottobre 2011, n. 4694, Casani, in *Dir. Pen. Cont*., 10 febbraio 2012, mentre per un contributo dottrinale R. BARTOLI, *L'accesso abusivo a un sistema informatico (art. 615-ter c.p.) a un bivio ermeneutico teleologicamente orientato*, in op. cit., p. 123 ss. e la nota a sentenza G. ROMEO, *Le Sezioni Unite sull'accesso abusivo a un sistema informatico o telematico*, in *Dir. Pen. Comp*., 2/2012. Per un esame completo della fattispecie di "*Accesso abusivo ad un sistema informatico o telematico*" tipizzata nel nostro codice penale all'art. 615-*ter* c.p., invece, 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 AA. VV (a cura di L. PICOTTI), *Tutela penale delle persone e nuove*, op. cit., pp. 125-155.

[172] Nonostante la possibilità, per gli Stati membri, di innalzare gli *standards* minimi di tutela previsti dalla direttiva, il legislatore nazionale ha mantenuto la condizione della violazione della misura di sicurezza. Tuttavia è doveroso evidenziare che l'art. 615-*ter* c.p. stabilisce la reclusione fino a tre anni per l'intruso informatico, superando quindi di un anno il *minimum* richiesto dall'art. 9 della direttiva in punto pena.

condotta di accesso al sistema informatico, a prescindere dall'eventuale impossessamento ed uso, da parte del soggetto agente, dei dati e dei programmi ivi contenuti[173].

Per quanto attiene all'*elemento psicologico* del reato, si è già detto come la direttiva prescriva che il soggetto agente debba essere animato dall'*intenzione diretta*, da interpretarsi alla stregua della tipologia di dolo che, nel nostro ordinamento, è dotata di maggiore intensità, ovverosia il *dolo intenzionale*.

I successivi artt. 4 e 5 disciplinano due fattispecie di *interferenza illecita* in relazione, rispettivamente, ai *sistemi* ed ai *dati*. Più precisamente, la prima disposizione punisce la condotta di ostacolare gravemente o di interrompere il funzionamento di un *sistema di informazione*, che può essere compiuta attraverso l'immissione nel sistema di dati informatici o attraverso la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati o, ancora, rendendo i dati inaccessibili. La seconda disposizione, invece, punisce in via autonoma le condotte d'interferenza relative ai *dati* (comunque compiute nel contesto di un sistema d'informazione), ovverosia la cancellazione, il danneggiamento, il deterioramento, l'alterazione, la soppressione o, infine, l'atto di renderli inaccessibili. Per entrambe le fattispecie di interferenza le condotte devono essere poste in essere «*senza diritto*» e, per quanto attiene all'elemento psicologico, *intenzionalmente*.

---

[173] Il tema è stato affrontato in relazione alla fattispecie prevista dall'art. 615-*ter* c.p. in Cass., pen., Sez. V, sent. 29 maggio 2008, n. 26707, Scimia, in *Foro it.*, II, 2009, p. 487 e s. e Cass. pen., Sez. VI, sent. 8 ottobre 2008, n. 39290, Peparaio, in *Cass. pen.*, 2009, pp. 2828 e ss., in cui i giudici concordano nel ritenere che l'accesso al sistema di informazione per il perseguimento di finalità illecite, da parte di colui che abbia titolo per accedervi, non configura il reato di cui all'art. 615-*ter* c.p. (l'autore della condotta risponderà solo degli altri reati eventualmente commessi grazie all'accesso). *Contra* Cass. pen., Sez. V, sent. 10 dicembre 2009, n. 2987, in cui si ritiene integrato il reato anche a fronte del comportamento di chi, pur autorizzato ad accedere al sistema, vi permanga per finalità estranee a quelle su cui si fonda l'autorizzazione.

2.2. I casi di non punibilità previsti dalla direttiva 2013/40/UE

La direttiva 2013/40/UE prevede alcuni casi in cui gli Stati sono dispensati dall'obbligo di incriminare le condotte tipizzate[174].

In principalità ci si riferisce ai cosiddetti casi di «minore gravità», la quale, a norma del Considerando n. 11 della direttiva, ricorre quando il danno causato dal reato o il rischio per gli interessi pubblici o privati (ad esempio per l'integrità di un sistema di informazione o per dati informatici, o per l'integrità, i diritti o altri interessi di una persona) dallo stesso derivante sia «insignificante o di natura tale da non rendere necessario imporre una sanzione penale entro i limiti di legge o stabilire una responsabilità penale». In altri termini i suddetti casi sono riconducibili alla carenza di offensività.

In secondo luogo, tra le cause di non punibilità e, più precisamente, tra quelle di non colpevolezza deve annoverarsi il caso in cui, pur essendo soddisfatti tutti i criteri oggettivi dei reati previsti nella direttiva, gli atti vengano posti in essere dal soggetto agente senza essere animato da dolo. In proposito il Considerando n. 17 della direttiva esemplifica il caso di colui che non sappia che l'accesso non è autorizzato (riconducibile più precisamente alla figura dell'errore *ex* art. 47 c.p.) e quello del soggetto investito, da parte di un'impresa, di un incarico di collaudo o di protezione dei propri sistemi di informazione, che non può compiere il proprio lavoro senza accedere al sistema forzandone le misure di sicurezza[175].

---

[174] Per un esame completo delle cause di non punibilità previste dalla direttiva 2013/40/UE si rinvia a S. CIVELLO CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione*, in *Dir. Pen. Comp*., 30.10.2013, pp. 5 e ss.

[175] R. MOORE, *Cybercrime: investigative high-technology computer crime*, LexisNexis Publication, 2005, pp. 24 e ss., in cui l'autore, nell'offrire una classificazione delle varie tipologie di *hackers* spiega che i «*white hat hackers»* (letteralmente *hackers* dal cappello bianco) sono coloro che agiscono animati dall'intento di riparare i danni e le falle nella sicurezza dei sistemi di informazioni. Ad essi si contrappongono i «*black hat kachers»* (letteralmente *hackers* dal cappello nero, anche detti *crackers*), che sono animati dall'intento di danneggiare o distruggere i sistemi di informazione. Per un contributo circa la classificazione delle condotte penalmente rilevanti degli *hakcers* si consiglia la lettura di I. SALVADORI, *Hacking, cracking e nuove forme di attacco ai*

2.3. Le circostanze aggravanti del reato di "Interferenza illecita" (art. 9 della direttiva 2013/40/UE) ed il mancato adeguamento, da parte del legislatore italiano, della risposta sanzionatoria per i corrispondenti reati

La direttiva 2013/40/UE, con particolare riferimento al reato di "*Interferenza illecita*" (art. 9), prevede dei casi di aggravamento della pena[176].

L'art. 9, par. 3 della direttiva stabilisce che gli Stati membri, nel caso in cui le condotte di interferenza illecita relative ai sistemi (art. 4) o ai dati (art. 5) - poste in essere intenzionalmente attraverso uno degli strumenti di cui al precedente art. 7[177] - colpiscano un numero significativo di sistemi d'informazione, sono tenuti ad assicurare una pena detentiva massima non inferiore a tre anni.

L'art. 9, par. 4, invece, impone agli Stati di stabilire una pena detentiva *non inferiore nel massimo a cinque anni* in tre diversi casi.

Il primo di questi ricorre qualora la condotta del succitato reato venga posta in essere nell'ambito di un'organizzazione criminale come, ad esempio, un'*associazione con finalità di terrorismo*[178]. Con riferimento a tale circostanza si segnala che, attualmente, il nostro ordinamento prevede l'aumento di pena, prescritto dalla direttiva esclusivamente per le organizzazioni di stampo mafioso, *ex* art. 7, co. 1, d.l. 13.5.1991, n. 152 (convertito in l. 12.7.1991, n. 203), recante

---

sistemi di informazione. Profili di diritto penale e prospettive de iure condendo, in *Ciber. Dir.*, 9/2008, pp. 344 e ss.

[176]Per un esame completo delle circostanze aggravanti previste dalla direttiva 2013/40/UE si rinvia a S. CIVELLO CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione*, op. cit., pp. 6 e ss.

[177] Tali strumenti possono consistere in un programma per computer, destinato o modificato al fine di commettere uno dei reati tipizzati dalla direttiva (art. 7, lett. a) o in una *password* di un computer, un codice d'accesso, o dati simili, che permettano di accedere in tutto o in parte ad un sistema d'informazione (art. 7, lett. b).

[178] Sorprendentemente la direttiva non fa alcun espresso riferimento alle associazioni con finalità di terrorismo, limitandosi a considerare genericamente le organizzazioni criminali. Diversamente la decisione-quadro 2005/222/GAI – che, come si è detto, è stata sostituita dalla direttiva del 2013 – evidenziava come i sistemi di informazione fossero sempre più frequentemente presi di mira precipuamente da attacchi con finalità terroristica (si veda sul punto il Considerando n. 2 della Decisione-quadro 2005/222/GAI).

"*Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa*"[179]. In particolare, la disposizione appena richiamata prevede che per i delitti punibili con pena diversa dall'ergastolo, commessi avvalendosi delle condizioni previste dall'art. 416-*bis* c.p. (ovverosia al fine di agevolare l'attività delle associazioni dallo stesso previste), la pena è aumentata da un terzo alla metà. Orbene, per quanto riguarda il novero dei reati informatici attualmente previsti dal nostro ordinamento, anche qualora ricorressero le condizioni *ex* art. 416-*bis* c.p., l'unica condotta ad essere punita in maniera adeguata agli *standards* dell'art. 9, par. 4, della direttiva sarebbe il "*Danneggiamento dei sistemi informatici*", in base al combinato disposto dell'art. 635-*quater* c.p. (o 635-*quinquies* c.p., qualora il sistema sia di pubblica utilità) e del citato art. 7, co. 1, d.l. 13.5.1991, n. 152, che permetterebbe di comminare fino a sette anni e mezzo di reclusione[180]. Relativamente al "*Danneggiamento dei dati*", invece, la normativa italiana vigente soddisfa gli obblighi europei solo nel caso di dati relativi a sistemi di pubblica utilità (*ex* art. 635-*ter* c.p.), mentre in tutti gli altri casi il giudice non potrà - anche avvalendosi dell'aumento di pena previsto dall'art. 7, co. 1, d.l. 13.5.1991, n. 152 - infliggere una pena detentiva superiore nel massimo a quattro anni e mezzo.

Sul punto si rende pertanto necessario novellare il codice penale al fine di adeguarsi agli *standards* europei.

Il secondo caso, contemplato dall'art. 9, par. 4, lett. b) della direttiva, ricorre qualora le condotte di interferenza illecita, relativamente ai sistemi di informazione (*ex* art. 4) e ai dati (*ex* art. 5), causino «gravi danni». Sul punto è necessario osservare che se, da un lato, è innegabile che il concetto di «gravi danni» sia affetto da genericità e indeterminatezza, dall'altro lato, è altrettanto

---

[179] Per un esame degli elementi essenziali e della *ratio* politico-criminale dell'aggravante *ex* art. 7 d.l. 13.5.1991, n. 152, si rinvia a E. RECCIA, *L'aggravante ex art. 7 d.l. n. 152 del 13 maggio 1991: una sintesi di "inafferrabilità del penalmente rilevante"*, in *Dir. Pen. Cont*., 2/2015, pp. 252 e ss.

[180] Per un caso di reato informatico posto in essere nel quadro di un'organizzazione criminale, si veda Cass. pen., Sez. V, sent. 16.4.2004, n. 17664, Aiello, in *Foro. it*., 2004, II, pp. 667 e ss.

vero che il legislatore italiano non può esimersi dall'intervenire rispetto alla fattispecie di cui all'art. 635-*bis* c.p., dedicato al "*Danneggiamento di informazioni, dati e programmi informatici"* (corrispondente alle ipotesi contemplate *ex* artt. 4 e 5 predetti), che prevede la pena della reclusione da sei mesi a tra anni.

In particolare, la modifica della previsione codicistica dovrebbe consistere nell'introduzione di un'*aggravante ad effetto speciale*, rispondente alle aspettative del legislatore europeo *ex* art. 9, par. 4, lett. b), atteso che sul punto il riferimento all'aggravante di cui all'art. 61, n. 7, c.p. si dimostra del tutto inadeguato[181].

3. Il contrasto preventivo degli attacchi ai sistemi informativi previsto dalla direttiva (UE) 2016/1148 (NIS)

A soli tre anni di distanza dalla direttiva 2013/40/UE, e precisamente il 6 luglio 2016, il Parlamento ed il Consiglio dell'Unione Europea hanno adottato la direttiva 2016/1148/UE, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. direttiva NIS[182]).

Giova preliminarmente osservare come l'atto normativo in questione confermi la necessità, già avvertita dal legislatore del 2013, di predisporre un'efficace strategia per la tutela di *nuovi beni giuridici* che, prescindendo da qualsiasi connotato informatico in senso stretto, possono ricondursi alla *sicurezza* di reti e sistemi informativi, da intendersi come luoghi in cui vengono trattati e scambiati dati ed informazioni[183]. Tuttavia la direttiva del 2016, pur essendo sostanzialmente volta alla tutela degli stessi beni giuridici presi in considerazione

---

[181] S. CIVELLO CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione*, op. cit., pp. 6-7, in cui l'autore aggiunge che sarebbe opportuno «richiedere un conseguente intervento sull'art. 635-*quater* c.p., che già prevede un massimo edittale di cinque anni di reclusione, in un'ottica di graduazione delle pene e coerenza del sistema sanzionatorio».

[182] NIS è acronimo di *Network and information security*.

[183] Sul punto si veda il Considerando n. 8.

dalla direttiva del 2013[184], si distingue nettamente dal precedente intervento normativo sotto il profilo della strategia da adottare per il contrasto dei *cybercrimes*.

Invero la direttiva NIS predispone un articolato sistema di prevenzione dei rischi e degli incidenti che possono interessare le reti ed i sistemi di informazione, prescindendo dall'introduzione di nuove fattispecie criminose e prescrivendo agli Stati l'adozione di sanzioni, che, sotto il profilo formale, hanno natura amministrativa[185]. La direttiva in parola si discosta così nettamente dalla strategia tradizionale per il contrasto dei *cybercrimes*, in accordo alla quale era imprescindibile l'adozione di misure di repressione, con la conseguente proliferazione di nuove fattispecie penali negli ordinamenti nazionali. L'approccio inaugurato dalla direttiva NIS per perseguire efficacemente tale obbiettivo è dunque marcatamente preventivo[186].

Procedendo all'esame della direttiva 2016/1148/UE, è opportuno evidenziare come, sin dal primo Considerando della stessa, il legislatore europeo riconosca che oggigiorno le reti, i sistemi ed i servizi informativi giocano un ruolo addirittura «*vitale*» nella società, con la necessità di renderli affidabili e sicuri (Considerando n. 1), atteso il crescente numero di «incidenti» e attacchi posti in essere ai loro danni (Considerando n. 2). La necessità di tutelare efficacemente i sistemi informativi è legata anche alle importanti implicazioni pratiche che gli stessi hanno nella vita dei cittadini dell'Unione, dal momento che svolgono un

---

[184] La direttiva 2013/40/UE, come si ricorderà, parlava più precisamente di «sistemi di informazione».

[185] Sul punto è opportuno evidenziare che le misure di prevenzione nell'ordinamento italiano, come si vedrà più ampiamente nel prosieguo della trattazione, pur avendo natura sostanzialmente penale, sono un istituto formalmente amministrativo. Per una qualificazione, in generale, della natura delle misure di prevenzione si rinvia a P. PITTARO, *La natura giuridica delle misure di prevenzione*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali*, Giappichelli, 2018, pp. 143 e ss.

[186] Sulla vocazione preventiva della disciplina prevista dalla direttiva NIS, si veda C. MARKOU, P. JOUGLEUX, T. E. SYNODINOU, T. PRASTITOU, *EU Internet Law in the Digital Era*, Springer International Publishing, 2019, p. 289, in cui si legge: «However the NIS Directive is focusing on essential services infrastructures that are depending on technology and attempts to ensure resilience to cyberattcks by including the requirement for prevention of incidents».

ruolo essenziale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone, incidendo profondamente rispetto al settore del mercato interno (Considerando n. 3).

Inoltre, come si è osservato in precedenza, il carattere deterritorializzato dei sistemi d'informazione – che per funzionare presuppongono l'esistenza di un unico grande spazio cibernetico comune - impone agli Stati membri di cooperare tra loro e con la Commissione europea, impegnandosi per la sicurezza anche oltre ai propri confini nazionali.

Il punto di partenza per l'instaurazione di un'efficace cooperazione è rappresentato dall'adeguamento, da parte degli Stati, dei livelli di sicurezza dei sistemi di informazione, che in alcuni ordinamenti restano ben al di sotto degli *standards* minimi richiesti dal diritto eurounitario. Invero, nel Considerando n. 5 della direttiva si denuncia espressamente l'insufficienza delle misure e delle capacità di cui gli Stati membri dispongono in materia, le quali non bastano a garantire livelli elevati di sicurezza nell'Unione. Le diversità che si registrano tra i singoli Stati, in punto di strategie predisposte e livelli di preparazione raggiunti, hanno comportato una controproducente frammentazione degli approcci nell'Unione in materia, che la direttiva si propone di combattere (Considerando n. 5).

L'attuazione della strategia delineata dalla direttiva non coinvolge limitatamente gli Stati ed i relativi apparati amministrativi, presupponendo la collaborazione degli operatori dei servizi essenziali e dei fornitori di servizi digitali, per promuovere una cultura della gestione dei rischi e garantire la segnalazione degli incidenti più gravi[187]. Sarà quindi ovviamente frequente il caso

---

[187] A norma dell'art. 4, n. 4 della direttiva in esame per «*operatore di servizi essenziali*» si intende il soggetto pubblico o privato (di un tipo di cui all'allegato II) che soddisfa i criteri di cui al successivo art. 5, par. 2, ovverosia: a) fornire un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; b) dipendenza del servizio fornito dalla rete e dai sistemi informativi; c) l'eventuale incidente deve avere effetti negativi rilevanti sulla fornitura del servizio. Per «fornitore di servizio digitale», invece, si intende (*ex* art. 4, n. 5) qualsiasi persona giuridica che fornisca un servizio digitale ovverosia qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi (*ex* art. 1, n. 1,

in cui si creino delle intersezioni fra soggetti pubblici e privati, specie nel caso in cui i primi si avvalgano dei servizi offerti dai secondi come fornitori di servizi digitali e, in particolare, dei cosiddetti «servizi della nuvola» (cioè di *cloud computing*)[188]. Infine, rileva evidenziare come la direttiva NIS, atteso il ruolo vitale delle reti e dei sistemi di informazioni di cui si è detto, coinvolge - nell'ottica di migliorare le capacità e le conoscenze cibernetiche degli Stati membri - anche la cosiddetta società civile, il settore universitario e, specificatamente, quello della ricerca.

Orbene, tutti questi soggetti pubblici e privati sono chiamati dal legislatore europeo a collaborare, per assicurare una risposta efficace rispetto alla sfida lanciata dal *cybercrime*, in materia di sicurezza delle reti e dei sistemi informativi, adottando un approccio comune a livello di Unione, con l'assunzione, da parte degli Stati membri, di disposizioni minime in materia di pianificazione e scambio di informazioni[189].

3.1. L'ambito applicativo della direttiva NIS e la definizione di «incidente» (art. 4, par. 7)

L'oggetto della direttiva NIS consiste precipuamente nello stabilire misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi

---

lett. b, direttiva 2015/1135/UE che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione).

[188] Per la definizione di «*servizi della nuvola*» si veda il Considerando n.17 della direttiva, in cui si spiega che il termine comprende tutti i servizi che consentono l'accesso ad un insieme scalabile ed elastico di risorse informatiche condivisibili. Queste ricomprendono reti, *servers,* applicazioni, infrastrutture e servizi cibernetici di vario genere. In particolare il termine «scalabile» si riferisce alle risorse informatiche che sono assegnate in modo flessibile dal fornitore di servizi nella nuvola, indipendentemente dall'ubicazione geografica delle risorse, per gestire le fluttuazioni della domanda. L'espressione «insieme elastico», invece, è usata per descrivere quelle risorse informatiche che sono fornite e diffuse in base alla richiesta, al fine di aumentare e ridurre rapidamente le risorse disponibili in base al carico di lavoro.

[189] Sul punto rileva osservare che, in ogni caso, a mente dell'art. 346, par. 1, lett. a) TFUE, nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza.

informativi nell'Unione europea, al fine di migliorare il funzionamento del mercato interno (art. 1, par. 1). In particolare per perseguire tale obbiettivo, la direttiva prescrive agli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi (art. 1, par. 2, lett. a), di istituire un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri (art. 1, par. 2, lett. b), di creare una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (c.d. rete CSIRT) (art. 1, par. 2, lett. c), di stabilire obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali (art. 1, par. 2, lett. d), nonché di designare le autorità nazionali competenti in materia di sicurezza della rete e dei sistemi informativi (art. 1, par. 2, lett. e)[190].

I paragrafi da 3 a 7 dell'art. 1, invece, si occupano di perimetrare il campo d'applicazione della direttiva. In particolare, il paragrafo 5 precisa che la

---

[190] Con riferimento alle disposizioni in parola, merita di essere evidenziato il frequente riferimento, in esse contenuto, al concetto di *fiducia*, la quale deve connotare il rapporto di cooperazione intercorrente fra gli Stati. Si riportano di seguito i passi delle disposizioni più rilevanti della direttiva NIS, in cui viene fatto riferimento al concetto di *fiducia*: il Considerando n. 2, riferendosi agli incidenti che colpiscono i sistemi di informazioni, prevede che essi possono, tra l'altro, «minare la *fiducia* degli utenti»; il Considerando n. 31 chiarisce che tra i principali obbiettivi perseguiti dal legislatore europeo, attraverso la direttiva NIS, figura quello di «migliorare il funzionamento del mercato interno creando un clima di *fiducia* e sicurezza»; l'art. 1, par. 2 prescrive che nell'oggetto della direttiva rientra l'istituzione di «un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la *fiducia* tra di essi» (lett. b) e la creazione di «una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della *fiducia* tra Stati membri e promuovere una cooperazione operativa rapida ed efficace» (lett. c). Per certi versi il richiamo alla *fiducia* potrebbe apparire fuori luogo in riferimento alla materia *de qua*, atteso che l'ambito d'applicazione della direttiva NIS presenta un alto tasso di informatizzazione e di cibernetica, che, come sostenuto in apertura di questo lavoro, tende a neutralizzare i rapporti sociali (reali). Ad ogni buon conto, il riferimento alla *fiducia* può comprendersi alla luce del Considerando n. 1 della direttiva, a cui si è già fatto cenno. Invero, come si è detto, le reti e i sistemi di informazione hanno ormai assunto un ruolo «*vitale*» rispetto ai rapporti interumani nella società attuale e, per tale ragione, anche le relazioni che si instaurano nel *cyberspace* devono essere rette dalla *fides*, dalla correttezza, dalla buona fede, nonché dalla solidarietà, ben noti all'ordinamento italiano. In particolare, sulle connessioni fra principio di buona fede e principio solidaristico si rinvia a C. RESTIVO, *Contributo ad una teoria dell'abuso del* diritto, Giuffrè, 2007, p. 205 e ss.; R. BIN, G. PITRUZZELLA, *Diritto Costituzionale*, op. cit., pp. 517 e ss.

condivisione dei dati per tutelare i sistemi di informazioni può avvenire solo nella misura in cui essa è necessaria ai fini dell'applicazione della direttiva[191].

La *ratio* della previsione, a dire il vero piuttosto laconica e a tratti tautologica, è chiaramente quella di garantire la riservatezza di informazioni e dati sensibili, tutelando allo stesso tempo la sicurezza e gli interessi degli operatori di servizi essenziali e dei fornitori di servizi digitali, i quali - nell'adempimento dei loro obblighi di notifica verso le amministrazioni statali - non sono tenuti a comunicare indiscriminatamente qualsiasi dato di cui siano entrati in possesso.

Una limitazione ancor più stringente all'applicazione della direttiva è contenuta nell'art. 1, par. 6, a norma del quale lo scambio dei dati non può prescindere dalla salvaguardia delle *funzioni essenziali dello Stato*, in particolare quelle attinenti alla tutela della *sicurezza nazionale* ed al mantenimento dell'*ordine pubblico*[192].

Infine l'art. 1, par. 7, in applicazione del principio *lex specialis derogat generalis*, stabilisce che, laddove un atto giuridico settoriale dell'Unione preveda a carico degli operatori di servizi essenziali o dei fornitori di servizi digitali particolari obblighi (specie in tema di notifica degli incidenti) volti a garantire la sicurezza delle reti e dei sistemi informativi, le disposizioni speciali dell'atto settoriale prevarranno su quelle generali della direttiva 2016/1148/UE nella

---

[191] Considerando n. 5 della direttiva: «Fatto salvo l'art. 346 TFUE, le informazioni riservate ai sensi della normativa dell'Unione e nazionale, quale quella sulla riservatezza degli affari, sono scambiate con la Commissione e con altre autorità competenti solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione della presente direttiva. Le informazioni scambiate sono limitate alle informazioni pertinenti e commisurate allo scopo. Tale scambio di informazioni tutela la riservatezza di dette informazioni e protegge la sicurezza e gli interessi commerciali degli operatori di servizi essenziali e dei fornitori di servizi digitali».

[192] Art. 1, par. 6 della direttiva NIS: «La presente direttiva lascia impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza, e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati».

misura in cui gli effetti delle prime siano almeno equivalenti agli effetti delle seconde[193].

Procedendo nell'esame della direttiva, l'art. 4 fornisce alcune importanti definizioni. Invero, a norma del paragrafo 1 della disposizione, per «*rete e sistema informativo*» può intendersi alternativamente: un sistema di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere i segnali (indipendentemente dal tipo delle informazioni trasportate) (art. 4, par. 1, lett. a); qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali (art. 4, par. 1, lett. b); gli stessi dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle precedenti lettere a) e b) (art. 4, par. 1, lett. c).

Alla luce della definizione appena riportata, rileva osservare come il legislatore del 2016, che ha accorpato i concetti di «*rete*» e di «*sistema informativo*»[194], abbia solo apparentemente riprodotto la definizione di «*sistema di informazione*» *ex* art. 2, lett. a) della direttiva 2013/40/UE.

Invero, a norma della disposizione da ultimo richiamata, sia le apparecchiature per il trattamento automatico dei dati sia questi ultimi sono parti integranti del sistema di informazione. Diversamente la definizione di cui alla direttiva 2016/1148/UE ammette che il sistema possa consistere alternativamente nelle apparecchiature o nei soli dati. Tale rilievo consente di evidenziare come il diritto eurounitario ritenga ormai completamente superata la fase informatica della rivoluzione digitale, con la necessità di tutelare nuovi interessi attinenti alla sicurezza e alla riservatezza dei *sistemi informativi* (non informatici), i quali

---

[193] I settori rispetto ai quali opera il principio di specialità di cui all'art. 1, par. 7 della direttiva sono numerosi. Tra questi figurano - per espressa previsione del legislatore del 2016 - il settore della fornitura di reti pubbliche di comunicazioni o di servizi di comunicazione elettronica accessibili al pubblico (ai sensi della direttiva 2002/21/CE) ed il settore dell'identificazione elettronica e dell'erogazione dei servizi fiduciari per le transazioni elettroniche nel mercato interno (ai sensi del regolamento 910/2014, che abroga la direttiva 1999/93/CE).

[194] Sotto tale profilo è opportuno ricordare come il legislatore della direttiva 2013/40/UE, invece, avesse ritenuto di mantenere distinti i due concetti, occupandosi di definire soltanto quello di «sistema di informazione».

possono consistere anche in complessi di dati o informazioni, a prescindere dal legame con l'*hardware*[195].

Tra le definizioni di maggior interesse di cui viene dato conto nell'art. 4 della direttiva NIS, emerge quella di «*sicurezza della rete e dei sistemi informativi*», che non postula l'adozione di forme di tutela repressive. Invero il concetto di *sicurezza*, proposto dalla direttiva in parola, fa riferimento alla capacità di resistere ad ogni azione che possa compromettere la *disponibilità*, l'*autenticità*, l'*integrità* o la *riservatezza* dei dati conservati, trasmessi o trattati attraverso le reti o i sistemi informativi (art. 4, par. 2).

La definizione a cui si è appena fatto riferimento emblematizza il cambio di prospettiva accolto dal legislatore europeo, il quale, con riferimento ai sistemi di informazione, sceglie di accantonare, come principale strumento di tutela - pur continuando a riconoscerne l'utilità - le misure di repressione, alle quali *preferisce quelle di prevenzione*. Invero lo stesso concetto di *resistenza* attiene alla capacità del sistema di sopravvivere ad eventuali attacchi attraverso il ricorso a misure che, intervenendo prima che si produca l'offesa, permettano di conservare intatte le funzioni essenziali dello stesso[196].

Particolare rilievo assumono infine i concetti di «*incidente*» (art. 4, n. 7) e di «*rischio*» (art. 4, n. 9). Quest'ultimo deve essere inteso come ogni circostanza o evento con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi.

---

[195] Sui nuovi interessi giuridici che, a seguito dello sviluppo cibernetico, sono divenuti meritevoli di tutela penale si consiglia la lettura di I. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico, una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, op. cit., pp. 149-155. In particolare l'autore, soffermandosi sulla fattispecie di *"Accesso abusivo ad un sistema telematico o informatico"*, ritiene non condivisibile la tesi della ricostruzione dell'interesse giuridico tutelando sia in termini di *domicilio informatico* sia in termini di *integrità dei dati e dei programmi informatici*. Invero, secondo Salvadori, l'interesse tutelando consiste nella *sicurezza* e *riservatezza dei dati e dei programmi* a prescindere dal loro "contenitore".

[196] Il concetto di *sicurezza* come *capacità di resistere* agli attacchi è divenuto, attraverso i successivi interventi normativi, elemento costituivo della «*resilienza*», della quale si parlerà più ampiamente nel prosieguo.

L'«incidente», invece, viene definito come ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi, il quale deve essere sottoposto ad un trattamento che comprenda tutte le procedure necessarie per la sua identificazione, analisi e contenimento (art. 4, n. 8). La direttiva richiede che gli incidenti – *rectius* i loro effetti negativi – siano connotati dal carattere della rilevanza. In altri termini essi devono presentare *concreta idoneità offensiva*, da valutarsi alla luce degli appositi criteri elencati nell'art. 6 della stessa, ovverosia:

a) il numero di utenti che dipendono dal servizio colpito dall'incidente;

b) la dipendenza dei settori di cui all'allegato II della direttiva da tale servizio[197];

c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;

d) la quota di mercato riconducibile al servizio colpito dall'incidente;

e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;

f) la capacità, da parte del soggetto erogante, di assicurare la continuità del servizio ad un livello sufficiente, tenendo conto della disponibilità di strumenti alternativi per la sua fornitura.

L'art. 6, par. 2 precisa che la valutazione della rilevanza degli effetti negativi dell'incidente deve essere effettuata considerando altresì «*fattori settoriali*», i quali - in assenza di ulteriori specificazioni - si ritiene vadano ricondotti a tutte quelle *condizioni spazio-temporali*, *sociali*, *politiche* e *culturali* capaci di influire sul settore colpito dall'incidente[198].

---

[197] I settori indicati nell'allegato II alla direttiva sono i *settori strategici* dello Stato, corrispondenti alle sue *fondamentali strutture* politiche, economiche, costituzionali, sociali e in particolare: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, sanità, fornitura e distribuzione di acqua potabile, infrastrutture digitali.

[198] È opportuno evidenziare che il Considerando n. 28 offre un'elencazione dei fattori che, per ogni singolo settore, consentono di valutare il carattere rilevante degli effetti negativi prodotti dall'incidente. Così, ad esempio, per quanto riguarda il settore dell'energia, il volume o la quota di energia nazionale prodotta; per quanto riguarda il settore dei trasporti (areo, marittimo e ferroviario), la quota di volume di traffico nazionale e il numero di passeggeri o di operazioni di

A ben vedere il concetto di *fattore settoriale* presenta delle interessanti analogie con i parametri della «*natura*» e del «*contesto*» di cui all'art. 1, par. 1, della decisone-quadro 2002/475/GAI sulla lotta contro il terrorismo, che si sono già esaminati[199]. Invero, come si ricorderà, i due parametri devono essere impiegati per la valutazione della sussistenza della *capacità di arrecare un «grave danno ad un Paese o ad un'organizzazione internazionale»*, la quale deve connotare in concreto la condotta affinché possa dirsi terroristica.

Alla luce dei rilievi appena svolti, emerge come in relazione al reato di cyberterrorismo, nel caso in cui venga commesso al fine di distruggere un sistema informativo dello Stato, l'accertamento della concreta idoneità offensiva delle condotte dovrà tenere conto sia dei criteri della *natura* e del *contesto* in ambito cibernetico (art. 1 della decisione-quadro del 2002) sia dei *parametri settoriali* previsti dall'art. 6 della direttiva NIS. Solo attraverso l'impiego di tutti questi indici l'interprete potrà valutare il superamento della *soglia della gravità* del *danno* da parte della condotta criminosa - sia sotto il profilo terroristico, sia sotto quello più specificatamente cibernetico - e quindi la sua offensività in concreto[200].

---

trasporto merci su base annua; per il settore bancario e dei mercati finanziari, la loro importanza sistemica in base alle attività totali o al rapporto tra queste e il PIL; per il settore sanitario, il numero di pazienti assistiti dal fornitore su base annua; per la produzione, il trattamento e la fornitura di acqua, il volume, il numero e i tipi di utenti riforniti, inclusi, ad esempio, ospedali, servizi pubblici, organizzazioni o persone fisiche, nonché l'esistenza di fonti idriche alternative per servire la stessa area geografica.

[199] I parametri della «*natura*» e del «*contesto*», come si è detto, sono elementi costitutivi della definizione di condotta con finalità di terrorismo *ex* art. 270-*sexies* c.p.

[200] La valutazione complessa di cui si è parlato rappresenta l'adeguamento al cyberterrorismo del *metodo* per la valutazione della concreta offensività delle condotte di terrorismo, elaborato dalla Cassazione (Cass. pen., Sez. VI, sent. 15 maggio 2014, n. 28009), già esaminato nel precedente capitolo (v. §. 6.2. del Capitolo I).

3.2. La strategia nazionale per la tutela preventiva della sicurezza della rete e dei sistemi informativi (art. 7 della direttiva NIS)

Il Capo II della direttiva NIS è dedicato ai *quadri nazionali per la tutela della sicurezza della rete e dei sistemi informativi* e prescrive agli Stati membri di adottare alcune misure per attuare la strategia europea volta al contrasto preventivo dei «rischi» che interessano la materia (art. 4, n. 9).

In particolare, il legislatore eurounitario prevede che gli Stati predispongano «obiettivi strategici» e «opportune misure strategiche e regolamentari», nonché un adeguato «quadro di *governance*» per il conseguimento dei primi, coinvolgendo soggetti pubblici e privati competenti (art. 7, par. 1, lett. b).

L'art. 7, par. 1, lett. f) della direttiva, poi, prevede che gli Stati membri si dotino di un «*piano di valutazione dei rischi*». In assenza di ulteriori definizioni normative, sembra ragionevole ritenere che la valutazione debba consistere in un *giudizio prognostico* suddiviso in due fasi, volto a stabilire se ricorra una circostanza o un evento con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi. La prima fase del giudizio, quindi, dovrebbe essere dedicata all'individuazione della possibile fonte dell'offesa, mentre la seconda alla valutazione della concreta pericolosità della fonte individuata.

I *quadri nazionali*, inoltre, devono prevedere l'indicazione di «programmi di formazione, sensibilizzazione, istruzione» e di «piani di ricerca e sviluppo» (art. 7, par. 1, lett. d, e). Trattasi di strumenti volti ad avviare un *processo educativo* che assicuri un uso consapevole e critico dei sistemi informativi e che assumono rilievo come misure di *prevenzione positiva* di tipo *sociale*, come si dirà. In tale contesto, la ricerca - specie quella svolta in ambito accademico - può dare un contributo decisivo all'indagine relativa alle fonti degli incidenti, nonché rispetto all'elaborazione di nuove misure per prevenirli[201].

---

[201] Per un esame del ruolo rivestito dai cosiddetti «*security researchers*» si consiglia la lettura di L. EDWARDS, B. SCHAFER, E. HARINJA, *Future Law, Emerging technology,*

La direttiva NIS, inoltre, prescrive agli Stati di istituire delle *strutture* che consentano di realizzare un'efficiente cooperazione a livello nazionale e transfrontaliero tra le Autorità competenti in materia di sicurezza dei sistemi informativi. Tra queste figurano i «*punti di contatto unico nazionale*» (art. 8), che devono essere dotati di adeguate risorse[202].

Altre strutture rilevanti sono i «gruppi di intervento per la sicurezza informatica in caso di incidente» (c.d. CSIRT[203]). A norma dell'art. 9 della direttiva, i CISRT monitorano, intercettano ed analizzano le minacce cibernetiche rivolte agli enti pubblici e privati, occupandosi di elaborare strumenti per il contenimento dei loro effetti dannosi[204].

---

regulation and ethics, Edinburgh University Press, 2020, pp. 157-158 e pp. 166-167, nonchè S. C. MCQUADE, *Encyclopedia of cybercrime*, op. cit., pp. 158-161, in cui l'autore compie una dettagliata panoramica circa gli studi, le ricerche e i sondaggi in materia di *cybercrimes* nel quarantennio compreso fra il 1970 ed il 2010.

[202] Art. 8, par. 5: «Gli Stati membri garantiscono che le autorità competenti e i punti di contatto unici siano dotati di risorse adeguate per svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei rappresentanti designati nel gruppo di cooperazione».

[203] Acronimo di *Computer Security Incident Response Team*.

[204] Per un esame delle funzioni del CSRIT in relazione alla strategia europea per la tutela della sicurezza dei sistemi informativi si rinvia a R. BRIGHI, P. G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, op. cit., pp. 18 e ss.; A. BHARDWAJ, V. SAPRA, *Security Incidents & Response Against Cyber Attacks*, Springer International Publishing, 2021, p. 3-4.; Z. FILEDS, H. PATRICK, B. VAN NIKERK (a cura di), *Cyber Law, Privacy, and Security*, IGI Global, 2019, pp. 883-891, in particolare il paragrafo *Cybersecurity Incident Management*, in cui gli autori evidenziano che: «A CSRIT would be able on a local level to protect the infrastructure and manage the secutiy incidents. One of the roles of a CSRIT is to promote and provide cybersecurity awareness training, if a CSRIT does not exist the there will be limited training and employees would not be prepared to recognize potential cybersecurity incidents and threats. […] The development of a CSRIT can increase the rapidity to which the organization is able to respond to cybersecurity incidents, attacks and malicious threats. It is vital to respond to cybersecurity incidents and investigate the incidents swiftly to stop disruption of the provision of public services. The key function of a CSRIT would play a reactive role in which it responds to cybersecurity incidents and threats that affect the organization's technology, process and people». Gli autori, nel definire il CSIRT ed elencarne puntualmente tutte le funzioni (principali e secondarie), confermano la centralità rivestita dall'organismo in parola con riguardo all'attuazione della strategia di prevenzione teorizzata nella direttiva NIS.

Conclusivamente si ritiene di dare conto degli obblighi che la direttiva pone a carico degli *operatori dei servizi essenziali* per il mantenimento di attività sociali o economiche fondamentali dello Stato (artt. 4, n. 4 e 5, par. 2), al fine di evitare che questo possa subire un grave danno a causa degli incidenti che interessano i sistemi informativi nazionali.

A norma dell'art. 14 della direttiva NIS, gli ordinamenti nazionali devono imporre agli operatori l'adozione di misure tecniche ed organizzative (di cui la direttiva non fornisce un elenco) idonee a prevenire gli incidenti e a minimizzarne l'impatto sui sistemi informativi[205]. L'obbiettivo che il legislatore intende perseguire è chiaro: assicurare che i sistemi da tutelare siano in grado di resistere agli attacchi, acciocché non si registrino interruzioni dei servizi essenziali.

Gli operatori, inoltre, sono tenuti a notificare al CSIRT, senza indebito ritardo, gli incidenti ai danni dei servizi essenziali prestati, purché abbiano un impatto rilevante[206]. La rilevanza dell'impatto deve essere valutata alla luce dei tre parametri elencati nell'art. 14, par. 4, ovverosia: il numero di utenti interessati dalla perturbazione del servizio essenziale, la durata dell'incidente e la sua diffusione geografica.

---

[205] L'art. 14, par. 2 della direttiva prevede che: «Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi».

[206] M. LUBERTO, *Gli obblighi dei fornitori di servizi di comunicazione elettronica in caso di violazione dei dati personali (data breach) ed il delitto di cui all'art. 168, D.Lgs. n. 196/2003*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, UTET, 2019, pp. 944-952. Sul punto è interessante notare come *ex* art. 14, par. 2, della direttiva la notifica a cui sono tenuti gli operatori dei servizi essenziali non possa esporli a maggiori responsabilità. Si tratta di una previsione la cui *ratio* sembra risiedere nell'incentivare la collaborazione da parte degli operatori – ferma la sussistenza di specifici obblighi a loro carico – evitando di gravarli con la previsione di ulteriori responsabilità.

4. Il regolamento (UE) 2019/881 (c.d. Cybersecurity Act): oggetto e ambito applicativo

La panoramica delle fonti eurounitarie che regolamentano le implicazioni giuridiche della cibernetica non può prescindere dall'esame del *Cybersecurity Act*, ovverosia il regolamento (UE) 2019/881 del 17 aprile 2019, relativo all'Agenzia dell'Unione europea per la cybersicurezza (ENISA) e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione[207]. Il regolamento definisce dettagliatamente le funzioni, i compiti e la struttura dell'ENISA - già istituita con regolamento 460/2004 - la quale tra i suoi compiti principali annovera l'attuazione della stessa direttiva 2016/1148[208]. L'analisi del *Cybersecurity Act* risulta dunque indispensabile per comprendere a pieno la strategia elaborata a livello eurounitario per il contrasto dei reati cibernetici – ed in particolare degli attacchi ai sistemi informativi – rappresentandone, anzi, la più recente evoluzione.

Preliminarmente all'esame delle singole disposizioni dell'atto normativo, è opportuno chiarire che l'oggetto del regolamento consiste nel garantire il buon funzionamento del mercato interno, perseguendo nel contempo un elevato livello di *cybersicurezza*, *cyberresilienza* e *fiducia* all'interno dell'Unione (art. 1, par. 1). A tal fine il legislatore europeo stabilisce anche il quadro per l'introduzione dei sistemi europei di certificazione della cybersicurezza (art. 1, par. 1, lett. a e b).

Quanto poi al perimetro applicativo, l'art. 1, par. 2 chiarisce che il regolamento fa salve le competenze degli Stati membri per quanto riguarda le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale, nonché le attività dello Stato nell'ambito del diritto penale.

---

[207] Il Regolamento del 2019 ha abrogato il Regolamento (UE) n. 526/2013 (c.d. «regolamento sulla cybersicurezza»).

[208] Sul punto si veda il Considerando n. 24 del regolamento 2016/881, in cui emerge che l'attuazione della direttiva 1148/2016 è uno dei principali compiti dell'ENISA nell'ottica di rafforzare la cyberresilienza: «Il compito di base dell'ENISA è promuovere l'attuazione coerente del pertinente quadro normativo, in particolare l'effettiva attuazione della direttiva (UE) 2016/1148 e degli altri strumenti giuridici pertinenti che presentano aspetti relativi alla cybersicurezza, che è essenziale per rafforzare la cyberresilienza […]».

4.1. La definizione europea di cybersicurezza come bene giuridico comune ai reati cibernetici (art. 2, n. 1 del Cybersecurity Act)

Il regolamento 2019/881 dedica l'art. 2 alla definizione di alcuni concetti rilevanti in relazione alla tutela dei beni giuridici offesi dai reati cibernetici.

In particolare, il *Cybersecurity Act* fa espresso rinvio alla direttiva NIS per definire i concetti di «*rete e sistema informativo*» (art. 2, n. 2), «*strategia nazionale per la sicurezza della rete e dei sistemi informativi*» (art. 2, n. 3), «*operatore di servizi essenziali*» (art. 2, n. 4), «*incidente*» (art. 2, n. 6).

Tuttavia il regolamento introduce anche nuovi concetti, fra i quali figura quello di «*cybersicurezza*», che, come si è detto, è il bene giuridico comune ai reati cibernetici.

A norma dell'art. 2, n. 1 del *Cybersecurity Act*, la *cybersicurezza* consiste nell'insieme delle attività necessarie per proteggere la *rete ed i sistemi informativi*, gli *utenti di tali sistemi* e le altre *persone interessate dalle minacce cibernetiche*.

La prima osservazione da compiere circa la definizione in parola attiene alle sue caratteristiche di genericità ed ampiezza (si pensi all'impiego del termine «*attività*»), che rispondono all'esigenza di ricomprendere tutte le misure - qualsiasi natura esse abbiano (penale o amministrativa) - finalizzate al contrasto degli attacchi cibernetici[209]. Ad essere più precisi, come si è detto, l'obiettivo del

---

[209] Cfr. R. BRIGHI, P. G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, op. cit., p. 24, in cui gli autori evidenziano come l'ampiezza della definizione europea di *cybersecurity* avrebbe la funzione di comprendere un perimetro di *rischi* e *incidenti* quanto più ampio possibile, senza limitazioni concettuali. Ad ogni buon conto, dall'esame della definizione prevista dall'art. 2, n. 1 del *Cybersecurity Act* emerge che il legislatore europeo sostiene l'opportunità che gli Stati membri contrastino i *cybercrimes* avvalendosi di uno *strumentario multilivello*. Tale concetto si riferisce ad un complesso di misure - sistematicamente disciplinato - di varia natura e, dunque, non solo di *repressione* ma anche (e soprattutto) di *prevenzione*. Queste ultime, pur essendo strumenti formalmente amministrativi, hanno natura sostanzialmente penale. Ebbene, nonostante le molteplici problematiche che sorgono nel nostro ordinamento in relazione alle misure di prevenzione, esse - come si vedrà nel successivo Capitolo III - consentono di assolvere efficacemente agli obblighi di protezione imposti dal legislatore europeo, senza distorsioni delle categorie tradizionali del diritto penale, le quali invece conseguono all'anticipazione (a tutti i costi) della soglia della punibilità, anche anteriormente al tentativo punibile.

legislatore europeo è *proteggere* i nuovi interessi giuridici cibernetici (riconducibili *ad unum* entro la cybersicurezza), intervenendo secondo un'ottica di *prevenzione* (dunque *ante delictum*) e comunque in modo tale da conservare intatte le funzioni delle reti e dei sistemi informativi nazionali (quali infrastrutture critiche) senza interruzioni, le quali arrecherebbero grave danno allo Stato.

Come è già stato evidenziato, il concetto di *sicurezza cibernetica* è più ampio rispetto a quello previsto dall'art. 4, n. 1 della direttiva 2016/1148[210]. Il primo, infatti, non interessa soltanto la sicurezza e la riservatezza della rete e dei sistemi informativi (corrispondenti alle componenti del *physical* e *logical layer* del *cyberspace*, secondo la struttura tripartita di Even e Siman-Tov). La cybersicurezza ricomprende anche la tutela degli *utenti* e delle *altre persone interessate* (ovverosia lo *human layer*) *che possono essere colpite dalle minacce informatiche*.

Alla luce di questa corrispondenza è allora possibile ritenere che la *cybersicurezza* rappresenti il bene giuridico comune ai *cybercrimes*, che assomma in sé gli interessi della «sicurezza e riservatezza dei sistemi informativi», dell'«autodeterminazione informativa» e dell'«*habeas data*» individuati dalla dottrina[211].

Quando gli attacchi cibernetici riguardano infrastrutture critiche dello Stato - il cui danneggiamento (per la natura ed il contesto delle condotte) può comportare un *grave danno* al Paese – e sono commessi per gli scopi previsti dall'art. 1 della decisione-quadro 2002/475/GAI, l'offesa alla *cybersecurity* proviene da atti di *cyberterrorismo*[212].

Per completezza di segnala che il quadro delle definizioni offerte dall'art. 2 del *Cybersecurity Act* ricomprende anche il concetto di «*sistema europeo di certificazione della cybersicurezza*». Quest'ultimo consiste in una serie di regole,

---

[210] Sul punto si veda il §. 3 di questo Capitolo.

[211] Per la definizione degli interessi giuridici richiamati si rinvia al §. 4.2. del precedente Capitolo I.

[212] Sul punto si rinvia al §. 5 del Capitolo I, ove, tra l'altro, si è individuata l'ulteriore finalità che può connotare il cyberterrorismo.

requisiti tecnici, norme e procedure, stabiliti a livello di Unione, volti a certificare o comunque valutare la conformità di specifici prodotti[213], servizi[214] e processi[215] della tecnologia dell'informazione e della comunicazione (TIC) - che sono parte integrante delle reti e dei sistemi informativi - agli *standards* di sicurezza europei. Nel caso in cui la suddetta valutazione dovesse concludersi con esito positivo, l'organismo competente, appositamente istituito presso gli Stati membri, è tenuto a rilasciare il «*certificato europeo di cybersicurezza*» (art. 2, n. 11)[216].

Il rilascio della certificazione, dunque, presuppone l'adozione e la corretta esecuzione di un complesso di *best practices*, le quali possono essere ricondotte nell'alveo delle misure di prevenzione positiva contro i *cybercrimes*, delle quali si parlerà diffusamente nel successivo Capitolo III.

4.2. L'evoluzione dell'Agenzia europea per la cybersicurezza: dal regolamento (CE) 460/2004 di istituzione al regolamento (UE) 2019/881 di riforma

Il regolamento (UE) 2019/881, come anticipato, dedica il Titolo II alla descrizione degli obbiettivi (art. 4), dei compiti (artt. da 5 a 12) e dell'organizzazione (artt. da 13 a 45) dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA), la quale è stata istituita con regolamento (CE) 460/2004 (abrogato dal regolamento 526/2013) per «assicurare un alto ed efficace livello di

---

[213] Il «prodotto TIC» (art. 2, n. 12) è un elemento o un gruppo di elementi di una rete o di un sistema informativo.

[214] Il «servizio TIC» (art. 2, n. 13) è un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi.

[215] Il «processo TIC» (art. 2, n. 14) è un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC.

[216] Il *Cybersecurity Act* dedica alla materia della certificazione l'intero Capo III (e precisamente gli artt. da 46 a 65), prevedendo una disciplina piuttosto dettagliata in ordine alla protezione dei dati trattati, al monitoraggio di eventuali vulnerabilità dei sistemi ed alla verifica della sicurezza dei prodotti, dei servizi e dei processi TIC.

sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione»[217].

Il *Cybersecurity Act* descrive dettagliatamente la struttura dell'ENISA e degli organi di cui essa si compone, ovverosia: un consiglio di amministrazione, un comitato esecutivo, un direttore esecutivo, un gruppo consultivo ed una rete di funzionari nazionali di collegamento (art. 13).

Il consiglio d'amministrazione è composto da un membro nominato da ciascuno Stato membro e da due membri nominati dalla Commissione europea, tutti con diritto di voto (art. 14, par. 1). Attraverso questa composizione gli Stati vedono garantita la loro rappresentanza in materia di cybersicurezza, attese le funzioni di cui tale organo è investito ed in particolare l'indicazione degli orientamenti generali del funzionamento dell'ENISA. Inoltre il consiglio di amministrazione si occupa di formulare il «progetto di documento unico di programmazione dell'ENISA» e di adottarlo, sentito il parere della Commissione (art. 24). Trattasi di una funzione assai rilevante, dal momento che il suddetto *documento* consiste nello strumento in cui vengono pianificate tutte le attività che l'Agenzia dovrà svolgere su base annuale e, in alcuni casi, anche pluriennale (art. 24, par. 1). Il «programma di lavoro», inoltre, contiene la descrizione delle risorse finanziarie ed umane assegnate a ciascuna azione, conformemente ai principi di formazione del bilancio dell'Agenzia. In ogni caso, il programma annuale può essere sempre oggetto di modifica - secondo lo stesso procedimento previsto per la sua adozione – la quale si rende necessaria qualora venisse assegnato un nuovo compito all'ENISA. Il consiglio di amministrazione adotta le proprie decisioni a maggioranza dei suoi membri. Tuttavia per l'adozione del documento unico di programmazione e del bilancio annuale è richiesta la maggioranza di due terzi dei membri del consiglio di amministrazione (art. 18, par. 1 e 2)[218].

---

[217] Art. 1, par. 1 del Regolamento (CE) n. 460/2004, rubricato "*Ambito d'applicazione*".

[218] Il consiglio di amministrazione è assistito da un comitato esecutivo, il quale consta di cinque membri nominati tra i componenti dello stesso consiglio di amministrazione (art. 19 del regolamento). Il comitato non ha esclusivamente funzioni assistenziali, tant'è vero che per ragioni di urgenza, a norma del par. 7 dell'art. 19, può prendere determinate decisioni provvisorie a nome del consiglio di amministrazione. Tali decisioni sono notificate senza ritardo al consiglio di

Tra gli aspetti più interessanti previsti dal *Cybersecurity Act* con riguardo alla struttura dell'ENISA figurano il *Gruppo consultivo* (art. 21), il *Gruppo dei portatori di interessi per la certificazione della cybersicurezza* (art. 22) e la *Rete dei funzionari nazionali di collegamento* (art. 23).

A norma dell'art. 21, par. 1, il *Gruppo consultivo* è composto da esperti riconosciuti, che rappresentano i pertinenti portatori di interessi di numerosi settori interessati dall'uso della cibernetica ed in particolare: i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, gli operatori di servizi essenziali, le autorità competenti, le organizzazioni europee di normazione, le autorità di contrasto e controllo preposte alla protezione dei dati, nonché – ed è questo l'aspetto più interessante - le piccole e medie imprese, le organizzazioni dei consumatori e persino gli esperti universitari in materia di cybersicurezza. Una diversa composizione, del resto, non potrebbe garantire l'efficace adempimento, da parte del gruppo, del suo compito nei confronti dell'Agenzia, il quale consiste nel fornire una consulenza completa in relazione a tutte le attività svolte dalla stessa.

L'art. 22 disciplina il *Gruppo dei portatori di interessi per la certificazione della cybersicurezza*, il quale, sebbene presenti una composizione per certi versi analoga a quella del comitato appena esaminato, è investito di peculiari funzioni. In particolare, il Gruppo si occupa di fornire consulenza alla Commissione (sulle questioni strategiche riguardanti la cybersicurezza) e all'ENISA (su questioni generali e strategiche concernenti i compiti della stessa in materia di mercato, certificazione della cybersicurezza e normazione).

Da ultimo, l'art. 23 del regolamento disciplina la *Rete dei funzionari nazionali di collegamento*, ovverosia una struttura - composta dai rappresentanti di ogni Stato appositamente designati - la quale agevola lo scambio di informazioni tra l'ENISA e gli Stati membri, oltre a sostenere l'Agenzia nella

---

amministrazione, il quale decide se approvarle o rigettarle entro il termine di 3 mesi dalla loro adozione.

diffusione, in tutta l'Unione, dei risultati e delle raccomandazioni frutto della sua attività.

Ferma la struttura attuale dell'ENISA di cui si è appena dato conto, pare opportuno offrire una sintesi delle evoluzioni disciplinari che hanno interessato l'Agenzia nel corso del tempo.

L'ENISA è stata istituita con il compito di assistere la Commissione e gli Stati membri su questioni connesse con la sicurezza delle reti e dell'informazione, per la *prevenzione* dei problemi che possono interessarle[219]. Tra i compiti dell'Agenzia, l'abrogato regolamento istitutivo prevedeva la promozione di una *nuova cultura della sicurezza* (sviluppando un alto livello di competenze), affinché la questione della *cybersecurity* fosse adeguatamente affrontata a livello europeo e nazionale.

Il principale obbiettivo dell'ENISA consisteva, a norma dell'art. 2 del regolamento 460/2004, nel prestare assistenza alle Istituzioni (in particolare alla Commissione), agli organismi dell'Unione ed agli Stati membri nell'attuazione delle politiche necessarie a soddisfare le prescrizioni legali e regolamentari in materia di sicurezza delle reti e dei sistemi informativi, contribuendo a migliorare e rafforzare la loro capacità di *rilevare* e *prevenire* i problemi e gli incidenti legati alla *sicurezza informatica*.

Tra i compiti dell'Agenzia, invece, il regolamento 460/2004 prevedeva l'aumento delle competenze degli Stati in campo tecnologico, attraverso l'organizzazione di esercitazioni su vasta scala (con cadenza biennale) denominate *Cyber Europe*, le quali, simulando attacchi cibernetici, offrissero ai Paesi membri la possibilità di misurarsi con situazioni di crisi, testando il livello raggiunto in materia di prevenzione e repressione dei *cybercrimes*[220]. A far data

---

[219] Art. 2, paragrafi 1 e 2 del regolamento (CE) 460/2004.

[220] C. CONCETTI, *ibidem*. Si segnala che l'ENISA provvede a formulare raccomandazioni politiche basate sul processo di valutazione delle esercitazioni e sugli insegnamenti tratti da queste ultime, in base ai quali, tra l'altro, organizza l'offerta formativa in materia di cybersicurezza, rivolta precipuamente ad enti pubblici. Attraverso queste attività l'Agenzia contribuisce allo sviluppo delle capacità degli Stati in ordine alla prevenzione dei *cybercrimes* (art. 6, lett. h).

dal 2010, l'ENISA ha organizzato complessivamente cinque esercitazioni. In particolare, in occasione della simulazione del 2010, è stato riprodotto un attacco volto ad interrompere l'interconnettività di internet tra tutti gli Stati partecipanti, i quali dovevano attivarsi per il ripristino della stessa. L'esercitazione del 2012, invece, ha simulato un attacco diretto alle infrastrutture di distribuzione di energia elettrica, al fine di interromperne le funzioni. *CyberEurope2012* è stata connotata dalla partecipazione di numerosi soggetti privati, esponenti del mondo industriale e della sicurezza informatica, i quali hanno significativamente contribuito all'innalzamento del livello di *know how* messo in campo. L'ultima esercitazione, che si è svolta nelle date del 6 e 7 giugno 2018 (c.d. *CyberEurope2018* o, più brevemente, *CE*2018), è consistita nella simulazione di una serie di *attacchi digitali e ibridi* posti in essere da un *gruppo terrorista*, volti a colpire direttamente i *sistemi critici* degli aeroporti ed in particolare i relativi dispositivi di sicurezza, con guasti ai macchinari per il *check-in* e agli altri *software* in uso al personale, nonché malfunzionamenti delle *apps* di viaggio installate sugli *smartphones* dei viaggiatori. L'esercitazione è proseguita con l'annullamento dei voli e con la rivendicazione dell'attacco da parte del gruppo terrorista, che nel frattempo aveva già iniziato a propagandare la sua ideologia, postando le immagini delle infrastrutture aeroportuali fuori servizio e decantando la propria impresa attraverso i *social networks* e altri mezzi di comunicazione. L'esercitazione programmata per il 2020 è stata rinviata al 2022 (a causa della pandemia da COVID-19) ed è consistita nella simulazione di un *attacco cibernetico* all'*infrastruttura critica sanitaria* - già stressata dall'emergenza pandemica - con attacchi ai sistemi informativi del servizio sanitario nazionale, del ministero della salute, degli ospedali e dei fornitori privati di servizi sanitari elettronici (comprese le assicurazioni sanitarie)[221].

[221] Per una descrizione dettagliata dell'esercitazione si rinvia alla lettura del relativo comunicato stampa pubblicato nel sito istituzionale dell'Agenzia per la cybersicurezza nazionale (ANC), disponibile al seguente link: *https://www.acn.gov.it/notizie/contenuti/cyber-europe-2022*.

Il regolamento (UE) 2019/881, abrogando il regolamento 526/2013 (a sua volta abrogativo del regolamento istitutivo 460/2004), ha apportato significative novità in relazione alla struttura, agli obiettivi ed alle funzioni dell'ENISA.

In primo luogo, è opportuno osservare che, differentemente da quanto previsto nei precedenti regolamenti, il *Cybersecurity Act* ha finalmente riconosciuto la centralità dell'Agenzia in materia di contrasto della criminalità cibernetica e, con essa, la sua piena autonomia[222]. Infatti, mentre in passato – come si è visto – all'ENISA era riservato il ruolo di gregario rispetto alla Commissione ed agli Stati membri, oggi essa persegue autonomamente l'obiettivo del raggiungimento di un *elevato livello comune di cybersicurezza*. A tal fine l'Agenzia sostiene attivamente il miglioramento della capacità degli Stati membri, delle Istituzioni e degli Organismi europei in tema di *rilevazione* e *prevenzione* degli incidenti futuri, attraverso la formulazione di pareri e la condivisione di competenze in materia di analisi delle minacce e di vulnerabilità dei sistemi[223]. Sul punto l'art. 4, par. 1 del regolamento, dedicato agli obbiettivi dell'ENISA, precisa che l'Agenzia opera come *centro di competenze nel campo della cybersicurezza* grazie alla sua *indipendenza*, alla *qualità scientifica e tecnica* delle consulenze e dell'assistenza fornite, alle *informazioni* che mette a disposizione, alla *trasparenza* delle procedure, ai *metodi operativi* utilizzati e alla *diligenza* nell'esecuzione dei suoi compiti.

Quanto ai compiti dell'ENISA, invece, essi vengono dettagliatamente descritti negli artt. da 5 a 12 del *Cybersecurity Act* e consistono in: sviluppo e attuazione delle politiche e della normativa dell'Unione (art. 5), sviluppo delle

---

[222] Secondo quanto previsto dall'art. 3, par. 3 del regolamento, l'ENISA, nello svolgimento dei suoi compiti, agisce in maniera indipendente, evitando nel contempo la duplicazione delle attività degli Stati membri e tenendo conto delle competenze degli stessi.

[223] Per quanto riguarda il ruolo di ENISA in materia di prevenzione degli incidenti si veda il Considerando n. 34 del *Cybersecurity Act*: «Nello svolgere il suo compito di sostegno della cooperazione operativa nell'ambito della rete di CSIRT, l'ENISA dovrebbe essere in grado di assistere gli Stati membri su loro richiesta, ad esempio fornendo consulenza su come migliorare le loro capacità di prevenzione e rilevazione degli incidenti e di risposta agli stessi […]»; nonché il successivo Considerando n. 36, in cui viene specificatamente previsto che il sostegno prestato da ENISA alle indagini tecniche, compiute dagli Stati *ex post* rispetto alla commissione del reato da cui dipende l'incedente occorso, deve essere incentrato sulla prevenzione degli incidenti futuri.

capacità (art. 6), cooperazione operativa a livello di Unione (art. 7), mercato, certificazione della cybersicurezza e normazione (art. 8), conoscenze e informazioni (art. 9), sensibilizzazione e istruzione (art. 10), ricerca e innovazione (art. 11) e cooperazione internazionale (art. 12).

Con riguardo al primo compito, l'Agenzia sviluppa e attua la normativa e le politiche europee in materia di cybersicurezza, anzitutto prestando assistenza e consulenza, sia a livello sovranazionale che nazionale[224]. In proposito l'art. 5, n. 2 del regolamento evidenzia come l'ENISA assista gli Stati peculiarmente nell'attuazione della direttiva (UE) 2016/1148, a riprova dello stretto legame intercorrente tra i due atti normativi sotto il profilo degli obiettivi da raggiungere in ambito di *cybersecurity*[225]. Invero, a mente degli obblighi in tema di notificazioni di cui all'art. 10, par. 3 della direttiva NIS, l'ENISA - secondo quanto prevede l'art. 5, n. 6 del regolamento - sostiene il riesame periodico delle attività politiche dell'Unione, attraverso la preparazione di una relazione annuale sulle notifiche degli incidenti trasmesse dagli Stati membri, dai prestatori di servizi fiduciari e dai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico.

L'art. 6 del regolamento, rubricato "*Sviluppo delle capacità*", è dedicato al compito più importante di cui è investita l'ENISA, ovverosia la *prevenzione dei cybercrimes* e in particolare del *cyberterrorism*. Invero, secondo la previsione in parola, l'ENISA assiste gli Stati membri e le Istituzioni dell'Unione nel

---

[224] Tali attività di assistenza e consulenza si rivolgono anche a politiche settoriali. Con particolare riguardo al settore delle comunicazioni elettroniche l'art. 5, n. 5 del regolamento prevede che l'ENISA sostiene: a) lo sviluppo e l'attuazione della politica dell'Unione nel settore dell'identificazione elettronica e dei servizi fiduciari, in particolare fornendo consulenza e emanando orientamenti tecnici e agevolando lo scambio di migliori pratiche tra le autorità competenti; b) la promozione di un livello di sicurezza più elevato delle comunicazioni elettroniche, anche fornendo consulenza e competenze e agevolando lo scambio delle migliori pratiche tra le autorità competenti; c) gli Stati membri nell'attuazione di aspetti specifici relativi alla cybersicurezza della politica e del diritto dell'Unione in materia di protezione dei dati e vita privata, anche fornendo su richiesta un parere al comitato europeo per la protezione dei dati».

[225] A norma dell'art. 5, n. 1 del regolamento, l'assistenza può consistere in pareri indipendenti, analisi, nonché in veri e propri lavori preparatori e orientamenti, al fine di fornire consigli e migliori pratiche su questioni quali la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni.

miglioramento della prevenzione e precisamente delle attività di rilevazione e analisi delle minacce e degli incidenti informatici, nonché nello sviluppo della capacità di reazione agli stessi.

Il compito relativo al miglioramento della prevenzione viene adempiuto attraverso lo sviluppo di veri e propri *piani strategici nazionali* – compatibilmente con i diversi ordinamenti - in tema di sicurezza delle reti e dei sistemi informativi (art. 7, par. 2, della direttiva 2016/1148), nonché promuovendo la diffusione di tali strategie in tutta l'Unione[226].

4.3. L'alfabetizzazione cibernetica come misura per la prevenzione dei reati cibernetici

Tra le maggiori novità introdotte dal *Cybersecurity Act* con riguardo alle attività ed agli obiettivi dell'ENISA, figura la creazione una *cultura della cibernetica* con azioni multisettoriali e multilivello. Il riferimento è alle previsioni di cui agli artt. 9, 10 e 11 del regolamento, le quali disciplinano le attività svolte dall'ENISA sotto il profilo della cultura e dell'educazione all'informatica ed alla cibernetica, sempre nell'ottica della prevenzione dei *cybercrimes*[227].

---

[226] Sul punto rileva osservare che l'Agenzia monitora sull'attuazione dei piani strategici nazionali, promuovendo l'adozione di linee guida e *best practises* (art. 6, lett. e).

[227] Se da un lato è auspicabile che l'ENISA e gli Stati membri riescano, quanto prima, nella lodevole missione di creare una *cultura cibernetica* a partire dagli utenti comuni, dall'altro lato non v'è chi non veda come i cybercriminali siano già accomunati, sotto il profilo psicologico, da una solida cultura ben radicata, sinanco con una «Hacker Ethic», nella quale si riconoscono alla stregua di eroi. Così S. C. MCQUADE, *Encyclopedia of cybercrime*, op. cit. pp. 87-88 e, conformemente, S. LEVY, *Hackers: Heroes of the Computer Revolution*, O REILLY, 1984, p. 40, J. I. ROSS, *Cybercrimes*, op. cit., p. 49, nonché, con particolare riferimento all'etica degli *hackers*, M. WEBB (foreword by C. DOCTOROW), *Coding democracy. How Hackers are distrupting power, surveillance and authoritarianism*, The MIT Press, 2020, pp. 1 e ss., in particolare il Capitolo "*The hacker ethic: Germany's chaos computer club and the genealogy of the hacker ethos*". Sull'importanza dell'adozione di piani educativi per i giovani da parte degli Stati, specificatamente al fine di prevenire i *cybercrimes* ed il cyberterrorismo, si veda S. C. MCQUADE, *Encyclopedia of cybercrime*, op. cit., pp. 144-145 e 151-154, in cui l'autore, ravvisando la necessità di una vera e propria «*digital youth culture*» - che dovrebbe diffondersi tra i giovani sin dall'età scolare - individua le tematiche che i suddetti piani educativi dovrebbero

L'art. 9, rubricato "*Conoscenze e informazioni*", spiega che l'ENISA monitora costantemente le tecnologie della cybersicurezza emergenti, valutandone l'impatto in ambito *sociale*, *giuridico*, ed *economico*[228]. L'Agenzia, inoltre, compie analisi strategiche con riguardo alle minacce e agli incidenti informatici, espressamente volte alla loro prevenzione (art. 9, lett. b). Sempre nell'ottica di contribuire a formare una solida cultura della cibernetica, l'ENISA si occupa di raccogliere conoscenze ed informazioni in materia di cybersicurezza - fornite dalle Istituzioni, dagli Organi dell'Unione, dagli Stati membri (su base volontaria), nonché dai portatori di interessi del settore pubblico e privato - che rende accessibili a chiunque, tramite un apposito portale dedicato.

L'art. 10 del regolamento, rubricato "*Sensibilizzazione e istruzione*", prevede che sia la stessa ENISA a dedicarsi alla sensibilizzazione dell'opinione pubblica circa i rischi connessi alla cybersicurezza ed a fornire orientamenti in materia di buone pratiche a favore degli utenti[229]. In particolare, l'Agenzia provvede a diffondere l'«*igiene*»[230], l'«*alfabetizzazione*»[231] e l'«*istruzione*» *informatiche*, proprio a partire dai cittadini (art. 10, lett. a e b).

---

affrontare. Inoltre cfr. J. I. ROSS, *Cybercrimes*, op. cit., p. 92-93, in cui l'autore evidenzia che «Unfortunately the average computer user and most criminal justice are inadequately prepared for detecting cybercrime and appropiately responding to allegations of cybercrime» e conclude sul tema augurandosi una maggior cultura della *cybersecurity* con l'organizzazione di corsi, laboratori e la pubblicazione di materiali aggiornati da parte delle Università e delle Agenzie del settore. Concordemente R. T. UDA, *Cybercrime, Cyberterrorism, and Cyberwarfare*, op. cit., p. 34-36, in cui l'autore ritiene opportuno estendere i percorsi formativi in materia di cyberterrorismo anche alle scuole medie inferiori e superiori.

[228] Con particolare riguardo a tale aspetto si segnala che, a norma dell'art. 9, lett. c) del regolamento, le valutazioni strategiche dell'Agenzia interessano, peculiarmente, la sicurezza della rete e dei sistemi informativi delle infrastrutture critiche, così come definite dalla direttiva 2016/1148.

[229] Tra i soggetti ai quali si rivolge l'attività di sensibilizzazione svolta dall'ENISA vanno ricompresi sia i singoli cittadini sia le organizzazioni e le persone giuridiche che forniscono servizi informatici (art. 10, lett. a del regolamento 2019/881).

[230] Per una definizione di «igiene informatica» o, meglio, *cibernetica* si rinvia a L. PUPILLO, *EU Cybersecurity and the Paradox of Progress,* in *CEPS policy paper*, 2021, pp. 6-7, in cui emerge che la cd. *igiene del computer* si sostanzia in *best practices* di *cybersecurity*, che dovrebbero diventare parte delle competenze quotidiane di ogni utente di Internet. Sulla stessa definizione cfr. A. JAMAL, H. JAHANKHANI, S. LAWSON, *Cybersecurity, Privacy and Freedom Protection in the Connected World*, Springer International Publishing, 2021, p. 294 e ss.,

in cui gli autori spiegano che i concetti di «igiene personale» e quello di «igiene cibernetica», in realtà, presentano numerose analogie, tanto che il secondo può essere letto alla luce del primo: «Cyber Hygiene is not much dissimilar to personal Hygiene. Often These two concepts are compared closely with each other. […] personal hygiene refers to maintaining health to prevent diseases. There are several factors involved in preventing the risk of spread, for example, environment, hand hygiene, sterilization, of equipment, disposal of waste etc. Similarly, Cyber Hygiene is related to the safety of data. The factors such as maintaining functional devices and updating necessary protective software are considered to prevent the risk of data loss or corruption». Inoltre cfr. I. CORRADINI, *Building a Cybersecurity Culture in Organizations*, Springer International Publishing, 2020, p. 106, in cui l'autrice definisce l'«igiene cibernetica» come: «broad concept referring to several activities to improve cybersecurity», aggiungendo, nella nota n. 4 di p. 106, che: «besides cyber hygiene other similar therms are used, like digital hygiene and cybersecurity hygiene». Alla luce dei succitati contributi dottrinali sembra ragionevole ritenere che per igiene cibernetica possa intendersi l'insieme delle misure e delle *best practices* che gli utenti del *cyberspace* possono adottare per migliorare la sicurezza *online* e mantenere integro il sistema secondo un approccio preventivo. Più latamente, tenuto conto del concetto di cultura cibernetica, l'*igiene digitale* potrebbe riferirsi alle modalità secondo cui l'utente si rapporta con il *cyberspace* e con i servizi che da esso dipendono, come per esempio l'uso degli stessi *social networks*. Conformemente M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds & Machines*, n. 29, Springer, 2019, p. 354, in cui emerge che la responsabilità legata alla garanzia di un adeguato livello di *igiene informatica*, che è presupposto per assicurare un «soddisfacente livello di robustezza dei sistemi» (il quale è un interesse comune), deve necessariamente ricadere sugli utenti e non su altri soggetti terzi. Infine, cfr. L. PUPILLO, *EU Cybersecurity and the Paradox of Progress,* op. cit., pp. 6-7, in cui l'autore evidenzia che la base giuridica, sulla quale (a livello domestico) dovrebbe fondarsi la responsabilità appena menzionata, consisterebbe nell'art. 122 Cod. Cons.

[231] Sul concetto di «*alfabetizzazione informatica*» si veda V. MIDORO, *Quale alfabetizzazione per la società della conoscenza?*, in *Italian Journal of Educational Technology*, 1.1.2007, disponibile al link: *https : / / www . provinz . bz . it / bildungsprache / sprachen / downloads / Quale _ alfabetizzazione _ per _ la _ soc . _ della _ conoscenza . pdf*, pp. 47-54, in cui l'autore propone la seguente definizione di alfabetizzazione: «abilità di usare il linguaggio per leggere, scrivere, ascoltare e parlare ad un livello adeguato per una società alfabetizzata (*literate society*), così da poter partecipare alla vita sociale» e conclude affermando che, al di là di una definizione stereotipata, è possibile evidenziare che l'«alfabetizzazione informatica» postula sei capacità: a) comprendere le caratteristiche dei documenti digitali (*media literacy*); b) scegliere le giuste applicazioni in relazione all'attività da svolgere; c) sapere usare le diverse applicazioni (ICT *literacy*); d) sapere risolvere problemi riguardanti la ricerca d'informazioni, usando metodi e strumenti per accedere all'informazione e alla conoscenza (*information problem solving, information literacy*); d) essere capace di condividere informazioni e conoscenze in un ambiente tecnologico (questa capacità è un prerequisito per realizzare un'intelligenza collettiva distribuita); e) capacità di partecipare alla vita di comunità costruendo conoscenza in ambienti virtuali, in modo cooperativo (lavoro cooperativo e apprendimento cooperativo in ambienti virtuali). Inoltre cfr. J. M. PEREZ TORNERO, *Understanding Digital Literacy*, Final report EAC/76/03, 2003 (al link: *https://www.researchgate.net/publication/271505720_Jose_Manuel_Perez_Tornero_Promoting_ Digital_Literacy*), p. 29, in cui l'autore propone la seguente definizione: «the acquisition of the technical competence for using information and communication technologies, understood in a

Il quadro delle disposizioni relative all'impegno dell'ENISA in ordine alla creazione di una cultura cibernetica, che consenta quantomeno di consapevolizzare i cittadini circa i *cybercrimes* ed i pericoli connessi all'utilizzo massivo e quotidiano della cibernetica, è completato dall'art. 11 del regolamento, dedicato alle attività di ricerca e innovazione svolte dall'Agenzia. Ebbene, per quanto riguarda questo settore, l'ENISA fornisce consulenze alle Istituzioni, agli organi dell'Unione ed agli Stati membri sulle esigenze e sulle priorità in materia di ricerca nel campo della cybersicurezza, al fine di consentire di reagire in maniera efficace ai rischi ed alle minacce informatiche attuali ed emergenti. Attraverso l'attività di ricerca l'Agenzia si propone di comprendere come impiegare le potenzialità delle nuove tecnologie cibernetiche per la prevenzione dei *cybercrimes* e, più in generale, dei rischi informatici (art. 11, lett. a).

---

broad sense, in addition to the acquisition of the basic practical and intellectual capacities for individuals to completely develop themselves in the Information Society». Per la definizione di «alfabetizzazione informatica» o «digitale» (*Digital Literacy*) che tenga conto degli effetti che essa può avere sotto il *profilo sociologico*, si rinvia a M. DURANTE, U. PAGALLO, *Manuale di informatica giuridica e diritto delle nuove tecnologie*, UTET, 2012, p. 531, in cui è interessante notare come l'autore evidenzi che l'alfabetizzazione digitale in Italia è un «traguardo neppur lontanamente raggiunto» e che il nostro Paese «è patria di un vero e proprio *cultural divide* in materia digitale». Tali considerazioni, del resto, trovano conferma nelle problematiche emerse in relazione alla cosiddetta didattica a distanza, alla quale è stato fatto recentemente ricorso durante la pandemia da COVID-19. Come noto la DAD, pur rappresentando l'unico strumento in grado di consentire di proseguire le lezioni nelle fasi più acute del contagio, ha evidenziato difficoltà - riscontrate da molti studenti - sia in relazione alla possibilità di connettersi alla rete, sia in relazione alle conoscenze minime per l'utilizzo dei *devices* necessari. Sullo stesso argomento cfr. C. SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, op. cit., p. 773, in cui si legge che, secondo l'autore, una piena «alfabetizzazione informatica» è auspicabile per colmare le disuguaglianze e le iniquità sociali, che rappresentano l'altra faccia dello sviluppo tecnologico; F. FEDERICI, A. ALLEGRIA, M. DI STEFANO, *Il diritto del web. Rete, Intelligence e Nuove Tecnologie*, Primiceri, 2017, p. 160, ove gli autori evidenziano come il principale interesse giuridicamente rilevante che la Repubblica deve perseguire attraverso l'«alfabetizzazione digitale» consista nell'eliminare il *cultural divide* tuttora presente in Italia in materia; M. N. CAMPAGNOLI, *Informazione, social network & diritto*, Key Editore, 2020,p. 43, nota 99; G. SARACENI, *Digital Divide e povertà*, in *Dirittifondamentali.it*, 2/2019, pp. 1-19.

5. La cyberresilienza dell'Unione europea: etimologia del termine

Tra i principali compiti dell'ENISA, a norma dell'art. 1, par. 1 del regolamento 2019/881 - figura il perseguimento di un elevato livello di «*cyberresilienza*», per rafforzare la quale è essenziale, in ogni caso, «l'effettiva attuazione della direttiva (UE) 2016/1148 e degli altri strumenti giuridici pertinenti che presentano aspetti relativi alla cybersicurezza»[232]. Tuttavia il *Cybersecurity Act* non fornisce una definizione del termine, onde pare doveroso interrogarsi sul significato che esso assume alla luce del quadro normativo descritto.

La parola «*resilienza*» è entrata prepotentemente nel nostro linguaggio quotidiano ormai da qualche anno. L'inizio della sua diffusione, ad essere più precisi, è coincisa con l'acuirsi del contagio da COVID-19, potendosi attestare con buona approssimazione al 2020. In tale contesto il termine ha assunto il significato comune di *resistenza*, talvolta addirittura quello di *coriaceità*, rispetto alle prove a cui il virus ha sottoposto la popolazione mondiale. Così, nel giro di pochi mesi, il termine ha conosciuto un enorme successo, assurgendo a titolo del documento predisposto dall'Italia per accedere ai fondi del *Next Generation EU* (NGEU)[233]. Il cosiddetto «*Piano di Ripresa e Resilienza*» si propone di organizzare l'impiego dei finanziamenti europei, destinandoli alla realizzazione di sei «missioni», corrispondenti ad altrettanti settori strategici per lo sviluppo dell'economia nazionale. Tra questi settori figura quello della *digitalizzazione*, che, con la destinazione di circa il 21% delle risorse complessivamente stanziate

[232] Considerando n. 24 del *Cybersecurity Act*.

[233] Il *Next Generation* EU, come noto, consiste nel pacchetto di sovvenzioni e prestiti - per un ammontare complessivo pari ad euro 750 miliardi - introdotto dall'Unione europea per rilanciare le economie nazionali dopo la pandemia, favorendone peculiarmente lo sviluppo sotto il profilo ecologico e soprattutto digitale. Sul punto si veda quanto pubblicato nel sito della Commissione europea *https://ec.europa.eu/info/strategy/recovery-plan-europe_it*.

in favore dell'Italia, risulta la missione più finanziata dopo la transizione ecologica (a cui è destinato circa il 31% delle risorse)[234].

Tuttavia oggi, nonostante il termine «resilienza» sia inflazionato, pare vi siano ancora incertezze in relazione al significato che esso assume con specifico riguardo al settore della cibernetica. Pare dunque opportuno premettere alcune considerazioni sotto il profilo etimologico, che consentano di indagare l'origine del termine.

Ebbene la parola «resilienza» deriva dal verbo latino «*resiliere*», che, essendo il composto del prefisso *re-* e del verbo «*salīre*»[235], veniva impiegato con il significato di «ritornare di colpo», «rimbalzare indietro» e, quindi, «ritirarsi», «contrarsi»[236]. Il verbo veniva dunque utilizzato per descrivere il comportamento di alcuni oggetti e corpi, che, in forza della loro elasticità, tendevano a rimbalzare o comunque, qualora sottoposti all'azione di una qualche forza, a modificarsi solo temporaneamente, salvo poi riacquistare la loro forma originaria. Il significato figurato del verbo, invece, suggeriva l'idea del farsi scivolare addosso le cose, senza rimanere condizionati da accuse, critiche o attacchi.

Nel passaggio dalla lingua latina a quelle italo-romanze, è sopravvissuto il participio presente «*resiliens*» e, quindi, *resiliente* - da cui appunto *resilienza* - del cui utilizzo sistematico nella lingua italiana vi è traccia soprattutto nella letteratura scientifica a partire dal XVII secolo, ove veniva impiegato per indicare la proprietà fisica, posseduta da alcuni corpi, consistente nel rendere possibile il rimbalzo degli oggetti e il riflettersi dei suoni.

---

[234] Sul punto si veda il *Piano Nazionale di Ripresa e Resilienza* disponibile al link *https://www.governo.it/sites/governo.it/files/PNRR.pdf*, pp. 86 e ss. con riguardo alla missione della digitalizzazione e p. 94 per quanto concerne la *cybersecurity*. Per una visione d'insieme circa gli obbiettivi del *PNRR*, con particolare riferimento al settore delle infrastrutture digitali del Paese, si consiglia la lettura di V. BONTEMPI, *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, Roma TrE-Press, 2022, pp. 23 e ss.

[235] L. CASTIGLIONI, S. MARIOTTI, *IL - Vocabolario della lingua latina*, op. cit., p. 1203, il verbo «*sălĭo, is, salui*, (rariss. *sălĭi*), *saltum, īre*, IV, 1. intr.: saltare, balzare […]».

[236] Ivi, p. 1265, il verbo «*rĕsĭlĭo, is, sĭŭi, sultum, īre*, IV, intr. (*re* e *salio*), 1. Saltar indietro […]; 2. ritornar di corsa, affrettarsi a retrocedere […]; 3. rimbalzare […] (n.d.r. in particolare) anche fig. *ab aliquo crimen resilit*, un'accusa rimbalza via da qualcuno, non lo tocca, Cic.; 4. ritirarsi, restringersi […]; 5. rinunciare, disdire […].

Successivamente, nel XVIII secolo, «*resilienza*» e «*resiliente*» sono stati utilizzati anche in ambito filosofico, per significare l'«elasticità respingente» delle passioni umane, nella quale si manifesterebbe l'incostanza e la mutevolezza dell'animo dell'uomo.

A partire dalla seconda metà del XX secolo, dopo un periodo di scarso utilizzo, il termine tornava a diffondersi per lo più in ambito giornalistico e letterario. Esso veniva inoltre impiegato in fisica per indicare la capacità di un corpo di assorbire energia - se sottoposto a deformazione elastica - per poi subito restituirla verso l'esterno[237].

Resilienza dunque non è meramente sinonimo di *resistenza*: il materiale resiliente non si oppone, né contrasta l'urto fino a spezzarsi, ma lo ammortizza e lo assorbe, all'uopo modificandosi (eventualmente anche riducendosi), in virtù delle proprietà elastiche e della duttilità che lo connotano, pur di conservare l'integrità delle proprie funzioni sino al momento in cui tornerà allo stato iniziale.

---

[237] Per un esame dell'impiego del termine «resilienza» nelle diverse fasi dell'evoluzione della lingua italiana si rinvia a S. CRESTI, *L'elasticità di resilienza*, Accademia della Crusca, 12.12.2014, (al link: *https://accademiadellacrusca.it/it/consulenza/lelasticit%C3%A0-di-resilienza/928*). Con particolare riferimento alle attestazioni dell'uso del termine registratesi nella lingua italiana in epoca successiva al 1700, l'autore riferisce che, dopo una lunga pausa, il termine riappare verso la seconda metà del XX secolo in abito giornalistico e pubblicitario - venendo ancora una volta impiegato per indicare le proprietà elastiche di una superficie - e in ambito letterario, ove il termine è legato all'«esperienza del respingere». Il riferimento è a P. LEVI, *Se non ora, quando?*, Einaudi, 1982, p. 139, in cui l'autore impiega il termine *resiliente* per indicare un corpo capace di allontanarne un altro: «Schiacciata sotto il peso del corpo mascolino, Line si torceva, avversario tenace e resiliente, per eccitarlo e sfidarlo». Infine l'autore, per spiegare la proprietà fisica della resilienza, ricorre all'immagine delle corde della racchetta da tennis. Invero queste si deformano sotto l'urto della pallina, accumulando energia che viene restituita subito nel colpo di rimando. Sul punto si veda anche *Dizionario delle Scienze fisiche Treccani*, la voce *Resilienza*, consultabile al link: *https://www.treccani.it/enciclopedia/resilienza_(Dizionario-delle-Scienze-Fisiche)*.

5.1. Il concetto di resilienza nell'attuale quadro normativo e socioculturale

Alla luce delle considerazioni appena svolte sotto il profilo etimologico, è ora necessario interrogarsi circa il significato che il concetto di resilienza assume oggi, decontestualizzato dal settore della fisica nel quale è stato originariamente impiegato.

A tal proposito è preliminarmente opportuno evidenziare che nell'epoca contemporanea, ritenuta da molti l'età della crisi, l'uomo vive una condizione di smarrimento, esito inevitabile della fiducia riposta nella cultura moderna, nella ragione strumentale della scienza e nella presunta indipendenza dell'individuo. L'ordine del mondo, ridotto alla rappresentazione del dato, si manifesta nell'informatizzazione telematica, che ha provocato una radicale esteriorizzazione del sapere rispetto al sapiente e ha condotto al tecnicismo cibernetico e burocratico delle istituzioni (che partecipano della Personalità dello Stato), con conseguente scomparsa dell'individualità e deresponsabilizzazione della persona in ogni campo dell'esperienza sociale[238].

Tale crisi del sapere si manifesta con particolare vividezza nel campo del diritto, ove il legislatore tende sempre più frequentemente a risolvere i casi controversi proposti dall'esperienza sociale in modo occasionale, attraverso il ricorso a leggi-provvedimento; la giurisprudenza diviene creativa, offrendo sentenze (*rectius* massime), che assurgono a fonti del diritto; il giurista appare incapace di andare oltre l'interpretazione della norma positiva o l'analisi della decisione giudiziale[239].

---

[238] J. F. LYTOARD, *La condizione postmoderna. Rapporto sul sapere*, Feltrinelli, 1985, pp. 12 e ss.

[239] F. CAVALLA, *Retorica giudiziale, logica e verità*, in *Retorica, processo, verità*, Franco Angeli, 2007, p. 84. Inoltre cfr. AA.VV., P. MORO (a cura di), *Il diritto come processo. Princìpi, regole e brocardi per la formazione critica del giurista*, Franco Angeli, 2014, p. 10, in cui si legge che: «La frammentazione del diritto in molteplici settori disciplinari, privi di comunicazione tra loro, ha trasformato la specializzazione in tecnicismo, assolutizzando l'efficienza e l'utilità delle decisioni del legislatore o del giudice, sempre più minuziose e disordinate, perché destinate a risolvere questioni particolari e contingenti. Il diritto è stato così abbandonato al potere legislativo e giudiziario, riducendo lo studioso ad un mero compilatore di

Anche il diritto, dunque, è in crisi e rischia di ridursi a rappresentazione esteriore del dato a causa di un'informatizzazione che ha reso il giurista telematico un autonoma della norma o, al più, un estensore della giurisprudenza, il quale utilizza il proprio sapere tecnico (basato sulla congettura e sulla programmazione) per interpretare o elaborare il diritto vigente attraverso l'utilizzo di basi di dati («giuritecnica»), del linguaggio informatico («legimatica») o di sistemi decisionali esperti («giuscibernetica»)[240].

Quale ruolo assume dunque la *resilienza* rispetto alla tutela penale, alla luce del contesto critico appena tratteggiato e delle considerazioni precedentemente svolte sotto il profilo etimologico?

Per essere resilienti non basta genericamente resistere.

Invero il concetto di *resilienza* sottende alla capacità di *sopravvivere* a crisi, avversità o a specifici attacchi, *conservando* intatta la *natura*, la *struttura* e le *funzioni essenziali* dell'oggetto materiale dei comportamenti illeciti – le quali possono coincidere con il bene giuridico tutelato[241] - anche a costo di una loro temporanea riduzione o compressione[242].

---

giurisprudenza e l'avvocato ad un mestierante del foro, mero conoscitore di formalismi procedurali e degli usi giudiziari. Questo atteggiamento superficiale ha condotto ad un diritto inesistente, ossia alla perdita d'identità del diritto vigente, che i giuristi pratici spesso presuppongono di conoscere, operando nel proprio mondo professionale senza bisogno di scoprirlo».

[240] AA.VV., P. MORO (a cura di), *Il diritto come processo. Principi, regole e brocardi per la formazione del giurista*, op. cit., p. 11. Sul punto cfr. anche AA.VV., P. MORO (a cura di), *Etica, informatica, diritto*, Franco Angeli, 2008, p. 14, in cui l'autore esamina il rapporto tra l'informatica ed il giurista, tenuto conto del *background* formativo che quest'ultimo possiede: «Da una parte, se proviene dal modello formativo teorico, il giurista informatico diventa interprete di norme giuridiche positive attraverso la ricerca e l'utilizzo di basi di dati dalle quali reperire giurisprudenza, legislazione e dottrina, svolgendo un'attività definibile come *giuritecnica*, ma anche elaboratore di norme attraverso l'uso del linguaggio informatico, ponendo in essere una tecnica indicabile come *legimatica*. Dall'altra parte, se proviene dal modello formativo partico, il giurista informatico diventa applicatore di norme giuridiche attraverso l'uso di sistemi decisionali esperti per pervenire alla formazione e alla modifica robotica di atti non solo amministrativi (come un certificato anagrafico) ma anche giurisdizionali (come un decreto penale di condanna), attuando una procedura riconoscibile come *giuscibernetica*».

[241] Sul punto, a titolo esemplificativo, si pensi al caso delle *infrastrutture critiche cibernetiche*. Queste vengono impiegate dallo Stato per provvedere all'*erogazione di servizi essenziali* per i cittadini, la quale - come si è sostenuto in precedenza - è pertanto espressione della

Per perseguire un obiettivo tanto ambizioso non basta contrastare l'attacco con interventi a posteriori - volti a reprimerlo con l'esercizio di una forza contraria e superiore - ma servono strumenti che consentano di intervenire prima della soglia del tentativo penalmente rilevante, per scongiurare la compromissione del bene tutelato.

Siffatti strumenti, che rispondono ad una *ratio* chiaramente preventiva, possono essere erogati solo sulla base di parametri obiettivi rivelatori della pericolosità del soggetto agente, da valutare in concreto. Diversamente si corre il rischio di applicare misure *ante delictum* dotate di una pervasività sostanzialmente pari a quella della pena, con violazione dei principi sintetizzati dai broccardi *nulla poena sine culpa* e, *a fortiori*, *nulla poena sine crimine*.

5.2. La resilienza in ambito cibernetico

A partire dal 2020, la crisi – che, come si è detto, sino ad allora era stata legata a questioni etiche, morali, culturali e, non da ultimo, giuridiche - ha assunto natura marcatamente sanitaria, a causa della pandemia da COVID-19, e, successivamente, diplomatica e militare, a seguito dell'invasione russa dell'Ucraina del 24 febbraio 2022.

---

sua Personalità (art. 270-*sexies* c.p.). Ebbene, dette infrastrutture possono essere l'oggetto materiale delle condotte terroristiche, con conseguente interruzione dei servizi erogati, e, quindi, offesa del bene giuridico della Personalità dello Stato, che trova una sua manifestazione nella suddetta erogazione.

[242] Cfr. S. CRESTI, *L'elasticità di resilienza*, op. cit., in cui l'autrice, dopo una lunga ricostruzione etimologica di *resilienza*, fornisce la seguente definizione del termine: «Resilienza assume un valore simbolico forte in un periodo in cui l'accesso interpretativo più frequente alla condizione economica, politica, ecologica mondiale è fornito da un'altra parola, *crisi*: lo spirito di resilienza rappresenta la capacità di sopravvivere al trauma senza soccombervi e anzi di reagire a esso con spirito di adattamento, ironia ed elasticità mentale». Particolarmente interessante sul punto anche A. ZOLLI, *Resilienza*, Rizzoli, 2017, *passim*, in cui l'autore ritiene che la resilienza consista nella capacità di un sistema, di un'impresa o di una persona di conservare la propria integrità ed il proprio scopo fondamentale di fronte a una drastica modificazione delle circostanze esterne.

In questo nuovo contesto critico, dai tratti tragicamente concreti, si è registrata una spinta verso il mondo *cyber*.

Per quanto riguarda il COVID, si pensi alla necessità, a fini di profilassi del contagio, di utilizzare i sistemi di comunicazione elettronica per potersi riunire virtualmente, le piattaforme di *e-commerce* per acquistare qualsiasi tipo di bene, i sistemi di pagamento *online* (e le criptovalute come strumento finanziario di investimento)[243].

Per quanto riguarda il conflitto russo-ucraino, invece, la cibernetica ha assunto rilievo, per la prima volta in modo concreto, come ulteriore dimensione bellica, complice il pregresso impegno dimostrato dai Paesi appartenenti ai blocchi indirettamente contrapposti – in particolare la Russia - nell'avvalersi della stessa, per cercare di influire a vario titolo sulla vita politica degli Stati avversari[244]. Si è così sentito parlare più frequentemente di guerra cibernetica o *cyberwar*, di *cyberattacks* e comunque dell'impiego dei *social media*, quantomeno a fini propagandistici[245].

---

[243] Sugli effetti della pandemia in materia di *cybersecurity* si veda R. BRIGHI, P. G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea,* op. cit., p. 20: «La pandemia da COVID-19, inoltre, ha imposto cambiamenti così repentini nel panorama tecnologico da indebolire le misure di sicurezza informatica esistenti; i cibercriminali hanno sfruttato la situazione di disagio collettivo, nonché di estrema difficoltà vissuta da alcuni settori – come quello della produzione dei presidi di sicurezza e della ricerca sanitaria – per colpire le proprie vittime con vettori di attacco personalizzati».

[244] Per un'interessante ricostruzione delle *cyber operations* compiute dalla Russia, con particolare attenzione per la cosiddetta "guerra ibrida" si rinvia a S. JASPER, *Russian Cyber Operations: Coding the Boundaries of Conflict*, Georgetown University Press, 2020, pp. 27 e ss.

[245] A. LAVORGNA, *Cybercrimes*, op. cit., pp. 169, in cui l'autrice evidenzia che la pervasività del *cyberspace* e l'inevitabile rilevanza delle tecnologie dell'informazione e della comunicazione rispetto alle istituzioni militari e civili ha aperto nuovi e, sino ad ora, sconosciuti scenari di guerra. L'autrice riporta poi alcuni recenti esempi di *cyberwar*: «Think, for instance of the Russian cyberwarfare between 2014 e 2017 after the outbreak of the war in eastern Ukraine: during the siege of the Donetsk airport, Russia was able to jam GPS, radios and radar signals, crippling communications and impeding Ukrainian troops from using radios and phones for hours at a time. The attacks in Ukraine have raised the concerns by international community on the potential vulnerabilities of critical infrastructure across industries […]». Per una disamina delle diverse forme che può assumere la *cyberwar* si consiglia la lettura di M. WEBB (foreword by C. DOCTOROW), *Coding democracy. How Hackers are distrupting power, surveillance and authoritarianism*, op. cit., pp. 139 e ss. Per un esame della guerra cibernetica combattuta mediante il virus "*Stuxnet*", invece, si veda L. EDWARDS, B. SCHAFER, E. HARINJA, *Future Law,*

Alla cibernetica hanno così iniziato a guardare con crescente interesse sia i potenziali *perpetrators* dei *cybercrimes*, ovverosia i soggetti agenti per lo più organizzati in associazioni, sia gli ordinamenti nazionali, chiamati per contro a predisporre un efficace sistema di misure per prevenire i reati in parola.

In questo contesto critico ha assunto centralità la «cyberresilienza», per definire la quale è indispensabile tenere conto delle questioni già emersi con riguardo al *cyberspace* ed ai *cybercrimes*.

Invero sul punto la dottrina ha evidenziato come la *cyberresilienza* non consista tanto nella capacità di un *sistema* di «riprendersi da un trauma», attività che cronologicamente interessa la fase successiva alla verificazione dell'evento dannoso del reato, ma postuli «caratteristiche di prevenzione e pianificazione», le

---

Emerging technology, regulation and ethics, op. cit., pp. 159-158. Inoltre cfr. R. BRIGHI, P. G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, op. cit., pp. 21-22, in cui gli autori spiegano che: «Una dimensione nuova e problematica è legata alle c.d. *Cyberwar* e alle guerre di informazioni (*information warefare*) dove il conflitto tra gli stati viene condotto con attacchi *cyber* verso sistemi informatici di varia natura, infrastrutture nazionali critiche e servizi il cui malfunzionamento produce disagi. Il controllo delle informazioni non riguarda solo l'ambito militare ma anche ambiti come l'economia, la politica e la vita sociale, attraverso *fake news* e *trolls* che propagano informazioni manipolate sulla rete e amplificate dai *social network*». Sullo stesso tema cfr. A. BONFANTI, *Attacchi cibernetici e cyber war: considerazioni di diritto internazionale*, in *Notizie di Politeia*, XXXIV, vol. 132, 2018, pp. 118-127 e F. RUGGE, *Mind hacking: la guerra informativa nell'era cyber,* in *Notizie di Politeia*, XXXIV, vol. 132, 2018, pp. 118-127. La rilevanza della cibernetica e, in particolare, dei *social networks* in ambito militare è confermata, tra l'altro, dall'approvazione, in data 4 marzo 2022, da parte della Duma russa, della legge sulla responsabilità penale per chi diffonde *fake news* sull'operato dell'esercito russo e per chi scredita le Forze Armate russe impegnate in quella che il Cremlino ha ribattezzato "operazione speciale" in Ucraina. Le pene previste variano da multe da 30.000 a 60.000 rubli (secondo il corso di cambio attuale, rispettivamente 300 e 600 euro). Nel caso di diffusione delle *fake news* usando la propria «posizione ufficiale» o «per profitto» o per «fomentare l'odio politico, ideologico, razziale, nazionale o religioso» è prevista la multa fino a 50.000 euro oppure la reclusione fino a 10 anni. Nel caso di «gravi conseguenze» della violazione della legge è prevista la reclusione da 10 a 15 anni. A soli 2 giorni dall'entrata in vigore della legge si contavano già almeno una sessantina di persone fermate e multate. Sul punto si consiglia la lettura dell'articolo intitolato "*Russia, a soli 2 giorni dall'approvazione della legge sulle fake news già 60 fermi*", disponibile al link: *https: / / www.rainews.it / articoli / 2022 / 03 / russia-a-soli-2 - giorni - dallapprovazione - della - legge - sulle – fake – news – sullesercito -gi-60-fermi-e16dc414-4198-4039-943b-f15dbb5aa9c3.html*, nonché G. URICCHIO, *Guerra Russia-Ucraina, l'intervento di Anonymous e la cybersecurity*, in *Altalex*, 1.3.2022, disponibile al *link*: *https : / / www . altalex . com / documents / news / 2022 / 03 / 01 / guerra – russia – ucraina – intervento – di – anonymous – e – la – cybersecurity*.

quali, invece, interessano la fase anteriore all'offesa e quindi alla commissione del reato. Dunque il concetto di resilienza non può esaurirsi in una prospettiva meramente difensiva o repressiva, presupponendo invece l'avvio di un «processo adattivo legato ad un cambiamento di contesto o di sistema, secondo una prospettiva proattiva»[246].

In altri termini, il concetto penalmente rilevante di *cyberresilienza* fa riferimento alla predisposizione di misure che, sulla base di criteri rispettosi del dei principi costituzionali, consentano di monitorare le multiformi minacce provenienti dal *cyberspace*, intervenendo prima della commissione del reato cibernetico, in modo tale da conservare integre le funzioni del sistema costituente l'*infrastruttura digitale critica dello Stato*, secondo la definizione prevista dall'art. 2, lett. a) della direttiva 2008/114/CE.

La migliore dottrina in materia ha proposto alcune definizioni di *cyberresilienza*.

Secondo Linkov e Kott essa consisterebbe nella capacità dei sistemi di *prepararsi* agli attacchi cibernetici, *assorbirne* le conseguenze avverse, *riprendersi* dalle stesse e *adattarsi* alle modifiche eventualmente prodotte dagli attacchi[247].

La definizione in parola è stata sostanzialmente ripresa dal gruppo di ricerca in materia di *cybercrimes* e *cybersecurity* che opera stabilmente presso

---

[246] B. LUCINI, *Cyber Resilience e Sicurezza (nazionale): aspetti e considerazioni*, in *ITSTIME*, 2.6.2020, disponibile al link: *https://www.itstime.it/w/cyber-resilience-e-sicurezza-nazionale-aspetti-e-considerazioni-by-barbara-lucini/*; M. T. PARACAMPO, *FinTech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli, 2017, p. 242 e C. CONCETTI, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, op. cit., pp. 38 e ss.

[247] A. KOTT, I. LINKOV, *Cyber Resilience of Systems and Networks*, Springer International Publishing, 2019, pp. 1-29, in particolare il Cap. I intitolato *Fundamental concepts of Cyber Resilience: Introduction and Overview*, in cui gli autori affermano che: «Cyber resilience refers to the ability of the system to prepare, absorb, recover and adapt to adverse effects, especially those associated with cyber-attacks». Nello stesso senso B. ZOU, P. CHOOBCHIAN, J. ROZENBERG, *Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies*, JTS, 2021, pp. 1-19; K. HAUSKEN, *Cyber resilience in firms, organizations and societies*, in *Internet of things*, 11/2020, p. 2.

il *National Institute of Standard and Technology* (NIST) statunitense[248], secondo il quale la cyberresilienza presuppone quattro azioni, ovverosia: *to anticipate*, cioè la capacità di anticipare la commissione delle condotte cibernetiche, intervenendo prima della consumazione del reato; *to withstand*, cioè la capacità di resistere agli stress, assicurando l'integrità delle funzioni del sistema ritenute essenziali; *to recover*, cioè la capacità di ripristinare le funzioni, possibilmente entro tempi ridotti, qualora non sia stato possibile evitare il prodursi dell'evento dannoso; e, infine, *to adapt*, ovverosia la capacità del sistema di sapersi adattare senza modifiche agli elementi essenziali[249].

Altri autori, pur condividendo la struttura quadripartita teorizzata da Kott e Linkov, hanno proposto un diverso concetto di cyberresilienza. Questa, secondo la dottrina più recente, non consisterebbe tanto in un insieme di capacità che devono connotare contemporaneamente uno stesso sistema, bensì in una successione cronologica di fasi, ciascuna delle quali caratterizzata dall'estrinsecazione di una

---

[248] Il *National Institute of Standard and Technology* (NIST) è l'Agenzia del Governo statunitense che si occupa della gestione delle tecnologie ed in particolare di quelle dedicate alla comunicazione. Per una descrizione delle attività («*functions*») svolte dal NIST in materia di *cybersecurity* e dedicate al contrasto dei rischi cibernetici si veda la pagina del sito dell'Agenzia al link: *https://www.nist.gov/cyberframework/online-learning/five-functions*. Le *functions* sono quattro e precisamente: *to identify, to protect, to detect, to respond, to recover*.

[249] Cfr. R. ROSS, V. PILLITTER, R. GRAUBART, D. BODEAU, R. MCQUAID, *Developing Cyber Resilient Systems. A Systems Security Engineering Approach*, vol. 2, Draft NIST Special Publication, 2019, p. 68, ove si legge che la *cyberresilience* è «the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources». Poco oltre gli autori, in relazione alle "entità" che possono essere resilienti nel senso predetto, aggiungono che: «This definition can be applied to a variety of entities including: a system; a mechanism, component, or system element; a shared service, common infrastructure, or system-of-systems identified with a mission or business function; an organization; a critical infrastructure sector or a region; a system-of-systems in a critical infrastructure sector or sub-sector; and the Nation». Dunque la cyberresilienza può interessare direttamente anche lo Stato (contribuendo a definirne la Personalità) o, meglio, le sue strutture critiche fondamentali. Si segnala che la definizione viene ripresa altresì in D. J. BODEAU, R. D. GRAUBART, R. M. MCQUAID, J. WOODILL, *Cyber Resiliency Metrics Catalog*, Mitre, 2018, pp. 1 e ss. e S. MITTAL, A. TOLK, *Complexity Challenges in Cyber Physical Systems. Using Modeling and Simulation (M&S) to Support Intelligence, Adaptation and Autonomy*, Wiley, 2019, pp. 296. Per un esame della definizione di cyberresilienza secondo una prospettiva che tenga conto delle ricadute dei *cybercrimes* sulla società si rinvia a I. LINKOV, J. M. PALMA-OLIVEIRA, *Resilience and Risk. Methods and Application in Environment, Cyber and Social Domains*, Springer Netherlands, 2017, pp. 386 e ss.

delle quattro capacità suddette. Così, ferma la fase iniziale di preparazione, ne seguirebbe una di assorbimento degli effetti dannosi del reato, quindi quella di ripresa e, infine, la fase di adattamento del sistema alle modifiche imposte dall'evento dannoso.

Secondo questa impostazione, la cyberresilienza consisterebbe in un *processo* o, addirittura, in un vero e proprio *metodo strumentale al trattamento degli incidenti cibernetici* che possono interessare i sistemi di informazione[250].

Tuttavia, sulla scorta di quanto emerso dall'esame delle fonti europee e dalla loro interpretazione, chi scrive ritiene che la concettualizzazione della resilienza cibernetica alla stregua di *metodo* (HAUSKEN) sia meno compatibile, con la *ratio* preventiva perseguita dal legislatore eurounitario, di quanto lo sia quella che descrive la resilienza cibernetica come *coacervo di capacità* (KOTT e LINKOV). Infatti, a ben vedere, il metodo tetrafasico presuppone che vi sia in ogni caso l'offesa (e, quindi, la commissione del reato), atteso che, dopo la seconda fase di assorbimento, esso prevede l'adattamento del sistema agli effetti dell'evento dannoso del reato. È dunque evidente come in tal modo venga frustrato l'obbiettivo di prevenzione tanto caro al legislatore eurounitario. Per questa ragione sembra potersi ritenere che la teoria che considera la cyberresilienza come metodo per processare gli incidenti cibernetici si adatti maggiormente ad una visione tecnico-ingegneristica, non anche a quella del giurista, che, in questo settore, è chiamato ad interrogarsi sulle misure più adatte per intervenire prima della commissione del reato cibernetico.

In ultima analisi, per dirsi effettivamente realizzato l'obiettivo dello *sviluppo* e del *miglioramento della cyberresilienza* rispetto ai *cybercrimes* (art. 4, par. 2) e quello della *prevenzione delle minacce cibernetiche* (art. 4, par. 5) sanciti dal Regolamento (UE) 2019/881, è dunque necessario che gli ordinamenti

---

[250] La teoria che considera la cyberresilienza alla stregua di un *metodo tetrafasico* è sostenuta in K. HAUSKEN, *Cyber resilience in firms, organizations and societies*, op. cit., p. 2 e V. ZEMBA (a cura di), *Defining, measuring, and enhancing resilience for small groups*, in *Safety Science*, 12/2019, pp. 603-616.

nazionali predispongano delle misure che assicurino, rispetto ad uno stesso sistema, la coesistenza delle quattro capacità indicate da Kott e Linkov contemporaneamente.

6. L'evoluzione della normativa europea in materia di lotta al terrorismo e alla radicalizzazione violenta: interazioni con la legislazione in materia di reati cibernetici

La strategia per il contrasto preventivo del terrorismo, inaugurata dal legislatore europeo a partire dal *Nine Eleven*, si è sviluppata lungo due diverse direttrici.

La prima di queste è stata connotata dalla previsione di nuove fattispecie di reato - in generale caratterizzate da una sensibile anticipazione della soglia della punibilità - per favorire l'armonizzazione delle norme di diritto penale in tutti gli Stati membri e rafforzare così i meccanismi di cooperazione giudiziaria e di scambio di informazioni. In particolare, attraverso la decisone-quadro 2002/475/GAI (successivamente modificata dalla Decisione quadro 2008/919/GAI), già esaminata, sono state introdotte la definizione di «atti terroristici» e alcune altre norme comuni di incriminazione delle condotte di terrorismo, onde l'atto in parola rientra, a pieno titolo, tra le iniziative afferenti alla prima direttrice. Nello stesso solco si colloca anche la decisione-quadro 2005/671/GAI, con la quale il legislatore europeo ha chiesto a ciascuno Stato membro di trasmettere le informazioni relative ai reati terroristici, commessi nei rispettivi territori nazionali, alle competenti Agenzie europee (in particolare Eurojust ed Europol) e agli altri Stati membri, per favorire la cooperazione per la prevenzione del fenomeno terroristico. Procedendo secondo l'odine cronologico, merita di essere qui ricordata anche la Convenzione del Consiglio d'Europa per la prevenzione del terrorismo del 16 maggio 2005, la quale, pur non facendo espresso riferimento a condotte terroristiche informatiche - né tanto meno cibernetiche - ha introdotto le fattispecie di *pubblica provocazione per*

commettere un reato terroristico (art. 5) e di *addestramento a fini terroristici* (art. 7). Nella stessa ottica di prevenzione si colloca anche la Direttiva (UE) 2015/849, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. Tuttavia l'atto normativo che, più recentemente, ha previsto l'introduzione di nuove fattispecie per il contrasto del *fenomeno terroristico anche online* è la Direttiva (UE) 2017/541, che, pur sostituendo la Decisione-quadro 2002/475/GAI, ne ha conservato molte previsioni.

La seconda direttrice, invece, è stata connotata dalla predisposizione di misure - per lo più aventi natura solo formalmente amministrativa - capaci di incidere in ambito sociale e culturale, per bloccare sul nascere il processo di *radicalizzazione violenta*. Quest'ultima è il presupposto imprescindibile per la creazione del *contesto* e per la definizione della *natura* che rendono le condotte con finalità di terrorismo capaci di arrecare grave danno al Paese preso di mira. Ebbene, la Commissione europea, con Comunicazione del 21 settembre 2005[251], ha formulato, per la prima volta, un espresso riferimento alla lotta alla radicalizzazione, quale parte integrante di un approccio globale di prevenzione del terrorismo, definendola come «fenomeno che vede persone abbracciare opinioni, vedute e idee che potrebbero portare ad atti terroristici quali definiti all'art. 1 della decisione-quadro 2002/475/GAI sulla lotta contro il terrorismo»[252]. Tra le iniziative dedicate alla prevenzione della radicalizzazione figura anche la

---

[251] Comunicazione della Commissione al Parlamento europeo e al Consiglio del 21.9.2005 (COM(2005) 313 definitivo) "*Reclutamento per attività terroristiche – Affrontare i fattori che contribuiscono alla radicalizzazione violenta*".

[252] R. PEZZUTO, *Contenuti terroristici on line: l'Unione europea lavora a nuove norme per prevenirne la diffusione*, in *Dir. Pen. Comp.*, 4/2019, p. 38. La *ratio* che ha animato l'adozione della Comunicazione consiste nella predisposizione di misure di prevenzione (anziché introdurre nuove fattispecie di reato), che, incidendo sotto il profilo storico, sociale, religioso e ideologico, consentano di impedire sul nascere qualsiasi forma di radicalizzazione. Questa peculiare forma di prevenzione, che potrebbe dirsi *sociale*, può essere attuata soltanto attraverso lo sviluppo di efficaci politiche di contronarrativa (attraverso il *web* ed i *social networks*), l'istruzione e la predisposizione di programmi volti a garantire ai soggetti più vulnerabili - siccome facilmente influenzabili dagli ideologismi terroristici (come ad esempio i più giovani utenti dei *social networks* o i detenuti) - il coinvolgimento nella vita sociale, l'occupazione, l'inclusione e l'integrazione all'interno della comunità di riferimento, l'uguaglianza di opportunità, la non discriminazione e, infine, il dialogo interculturale.

Comunicazione del 15 gennaio 2014, con la quale la Commissione europea ha indicato ai Paesi membri un vero e proprio *elenco di priorità*, tra le quali figurano la *valorizzazione delle attività della Rete per la sensibilizzazione in materia di radicalizzazione*[253], la *formazione degli operatori che lavorano con individui a rischio* e la *diffusione di messaggi volti a destrutturare la propaganda terroristica*. La centralità assunta dalla materia della prevenzione del terrorismo e dell'estremismo violento è stata confermata dal suo inserimento tra le sfide più urgenti - insieme alla lotta alla criminalità organizzata e a quella informatica - dell'Agenda europea sulla sicurezza per il quinquennio 2015-2020. Il 25 novembre 2015, anche il Parlamento europeo ha adottato una risoluzione sulla prevenzione della radicalizzazione e del reclutamento di cittadini europei da parte di organizzazioni terroristiche, aggiornando la definizione di radicalizzazione quale «fenomeno che vede persone abbracciare opinioni, pareri e idee intolleranti suscettibili di portare all'estremismo violento»[254]. Da ultimo, le Istituzioni europee hanno approvato il Regolamento (UE) 2021/784 (in vigore a partire dal 7 giugno 2022), con il quale si mira a contrastare l'utilizzo illecito di Internet a fini di reclutamento, sostegno e celebrazione delle attività terroristiche, attraverso la riduzione della presenza di materiale propagandistico di carattere terroristico *on line*. Questo intervento normativo, sebbene dedicato specificatamente a contrastare la pubblicizzazione di contenuti terroristici attraverso gli strumenti cibernetici, dimostra come il legislatore europeo abbia finalmente preso consapevolezza, almeno in parte, dell'autonomia e della rilevanza che, sotto il profilo penale, hanno raggiunto le condotte frutto dell'interazione tra terrorismo e *cybercrime*.

---

[253] Tale obbiettivo deve essere perseguito attraverso il *Radicalisation Awareness Network* (RAN), ovverosia il centro di eccellenza, istituito nel 2011 e composto da 700 esperti provenienti da tutta Europa, che si occupa dello scambio di idee e progetti per un efficace contrasto dei fenomeni di radicalizzazione.

[254] Sul punto si veda il Considerando lett. b) della *Risoluzione del Parlamento europeo sulla prevenzione della radicalizzazione e del reclutamento di cittadini europei da parte di organizzazioni terroristiche* del 25 novembre 2015 (2015/2063(INI)) (2017/C 366/08), in G. U. UE 27.10.2017 – C366/101.

Così ripercorsa la sequenza degli interventi più rilevanti adottati dal legislatore eurounitario in materia di *prevenzione del terrorismo*, si ritiene opportuno concentrarsi sull'analisi della direttiva (UE) 2017/541 e del regolamento (UE) 2021/784, i quali, ciascuno per la direttrice d'appartenenza, rappresentano gli atti più recenti.

6.1. Il connubio fra Internet e terrorismo: le fattispecie previste dalla direttiva (UE) 2017/541 per contrastare il fenomeno

La direttiva (UE) 2017/541 del 15 marzo 2017, che sostituisce la decisione quadro 2002/475/GAI[255], stabilisce norme minime relative alla definizione dei

[255] Sui rapporti fra la decisione-quadro 2002/475/GAI e la direttiva (UE) 2017/541 si veda S. SANTINI, *L'Europa compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, in *Dir. Pen. Comp*., 7-8/2017, p. 14, in cui l'autore, riferendosi alla direttiva, precisa che: «Innanzitutto, l'intervento mira a colmare le lacune presenti nella decisione quadro 2002/475/GAI sulla lotta contro il terrorismo – così come aggiornata dalla decisione quadro 2008/919/GAI – alla luce della Risoluzione 2178(2014) del Consiglio di Sicurezza delle Nazioni Unite e del Protocollo addizionale alla convenzione del Consiglio d'Europa per la prevenzione del terrorismo, siglato a Riga il 22 maggio 2015, attraverso l'introduzione di quattro nuovi obblighi di incriminazione: la *ricezione di addestramento*, i *viaggi*, l'*organizzazione* o *agevolazione di viaggi a fini terroristici*; infine, il finanziamento del terrorismo». Ad ogni modo giova osservare come l'art. 3 della direttiva del 2017, nel definire i reati di terrorismo, richiami sostanzialmente la definizione contenuta nell'art. 1 della decisone-quadro del 2002, che la direttiva ha sostituito. In particolare, sotto il profilo oggettivo, gli atti terroristici possono così consistere in: a) attentati alla vita di una persona che possono causarne il decesso; b) attentati all'integrità fisica di una persona; c) sequestro di persona o cattura di ostaggi; d) distruzioni di vasta portata di strutture governative o pubbliche, sistemi di trasporto, infrastrutture, compresi i sistemi informatici, piattaforme fisse situate sulla piattaforma continentale ovvero di luoghi pubblici o di proprietà private che possono mettere in pericolo vite umane o causare perdite economiche considerevoli; e) sequestro di aeromobili o navi o di altri mezzi di trasporto collettivo di passeggeri o di trasporto di merci; f) fabbricazione, detenzione, acquisto, trasporto, fornitura o uso di esplosivi o armi da fuoco, comprese armi chimiche, biologiche, radiologiche o nucleari, nonché ricerca e sviluppo di armi chimiche, biologiche, radiologiche o nucleari; g) rilascio di sostanze pericolose o il cagionare incendi, inondazioni o esplosioni i cui effetti mettano in pericolo vite umane; h) manomissione o interruzione della fornitura di acqua, energia o altre risorse naturali fondamentali il cui effetto metta in pericolo vite umane; i) interferenza illecita relativamente ai sistemi, ai sensi dell'art. 4 della direttiva 2013/40/UE del Parlamento e del Consiglio nei casi in cui si applica l'art. 9, par. 3 o l'art. 9, par. 4, lett. b) o c), di tale direttiva in questione e interferenza illecita relativamente ai dati, di cui

reati terroristici e delle relative sanzioni ed è tesa all'armonizzazione degli ordinamenti nazionali in ambito penale, nell'ottica della creazione di un quadro giuridico comune che favorisca la cooperazione tra gli Stati - nonché tra questi e le competenti Agenzie europee - per il contrasto del terrorismo[256]. Inoltre, con la direttiva in esame, il legislatore ha inteso promuovere l'adozione di misure di protezione, sostegno e assistenza per le vittime del terrorismo, alle quali è dedicato il Titolo V della direttiva e, in particolare, gli artt. da 24 a 26.

Le basi giuridiche poste a fondamento della direttiva sono dunque due. Da un lato figura l'art. 83 TFUE che, come noto, consente al Parlamento europeo e al Consiglio di stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave, che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni, tra i quali rientra esplicitamente il terrorismo. Dall'altro lato figura l'art. 82, par. 2, lett. c), TFUE,

---

all'art. 5 di tale direttiva nei casi in cui si applica l'art. 9, par. 4, lett. c), di tale direttiva; j) minaccia di commettere uno degli atti elencati alle lett. da a) a i). Le finalità che possono connotare in senso terroristico uno degli atti appena elencati, invece, possono alternativamente consistere in: a) intimidire gravemente la popolazione; b) costringere indebitamente i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto; c) destabilizzare gravemente o distruggere le strutture politiche, costituzionali, economiche o sociali fondamentali di un paese o di un'organizzazione internazionale.

[256] Per completezza si segnala che la direttiva prevede l'introduzione di otto fattispecie di reato, ovverosia: "*Pubblica provocazione per commettere reati di terrorismo*" (art. 5), "*Reclutamento a fini terroristici*" (art. 6), "*Fornitura di addestramento a fini terroristici*" (art. 7), "*Ricezione di addestramento a fini terroristici*" (art. 8), "*Viaggi a fini terroristici*" (art. 9), "*Organizzazione o agevolazione di viaggi a fini terroristici*" (art. 10), "*Finanziamento del terrorismo*" (art. 11), "*Altri reati connessi ad attività terroristiche*" (art. 12). Alcune di queste, pur non essendo completamente nuove (siccome già previste dalla decisone-quadro 2002/475/GAI), sono state "aggiornate", tenendo conto degli sviluppi tecnologici e in particolare cibernetici, che il terrorismo ha saputo sfruttare. Sul punto A. LAVORGNA, *Cybercrimes*, op. cit., p. 179, in cui si legge che «There is no doubt that cyber-technologies are influencing how terrorist behave. As many other entities do, terrorist groups use the internet to secure many of their organisational goals through more efficient means». Nel prosieguo della trattazione ci si occuperà dunque delle fattispecie più rilevanti per il contrasto del fenomeno cyberterroristico, ovverosia quelle previste ai succitati artt. 5, 7 e 8.

che consente ai medesimi organi di stabilire norme minime sui diritti delle vittime della criminalità[257].

L'adozione delle misure previste dalla direttiva in parola si è resa necessaria in ragione della rapida evoluzione conosciuta dal fenomeno terroristico e del crescente numero di *foreign fighters*, ovverosia cittadini europei che - ancorché privi di una benché minima formazione in ambito militare - si arruolano nelle file delle organizzazioni terroristiche, per poi fare ritorno in patria, ove cimentarsi, spesso come *lupi solitari*, nella commissione di attentati[258].

Attraverso la direttiva (UE) 2017/541 il legislatore europeo, per la prima volta, riconosce piena autonomia alle *condotte terroristiche commesse attraverso l'uso di Internet* e in particolare dei *social networks*, prescrivendo che gli ordinamenti nazionali provvedano alla loro tipizzazione, con la previsione di adeguate risposte sanzionatorie[259]. *Facebook*, *Instragram*, *Tweeter* e le altre piattaforme che consentono di socializzare virtualmente sono finalmente riconosciute quali strumenti dotati di particolare pervasività, che possono essere impiegati abusivamente dai terroristi per perseguire le loro finalità.

---

[257] S. SANTINI, *L'Europa compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, op. cit., p. 14.

[258] Considerando n. 4 della direttiva 2017/541, in cui si legge che: «Negli ultimi anni, la minaccia terroristica è cresciuta e si è evoluta rapidamente. Persone indicate come *combattenti terroristi stranieri* si recano all'estero a fini terroristici. I combattenti terroristi stranieri che rientrano in patria rappresentano una minaccia accresciuta per la sicurezza di tutti gli Stati membri. Combattenti terroristi stranieri sono risultati implicati in recenti attentati e complotti in diversi Stati membri. Inoltre l'Unione e gli Stati membri fanno fronte a crescenti minacce rappresentate da individui che sono ispirati o istruiti da gruppi terroristici all'estero ma che rimangono in Europa». Per un esame del fenomeno dei *foreign fighters* si rinvia a L. MARINI, *Foreign terrorist fighters: verso la revisione della risoluzione 2178 (2014)*, in *Dir. Pen. Comp*., 20.12.2017, pp. 4 e ss., in cui l'autore propone una differenziazione dei *foreign fighters* in «*returnees*» e «*relocators*». I primi sono coloro che lasciano le aree di combattimento per far rientro nei propri Paesi di residenza o di nazionalità. I secondi, invece, sono coloro che, abbandonate le aree di combattimento, si dirigono verso altri Paesi, diversi da quelli di origine. Tale nuova destinazione, segnala l'autore, può essere frutto di una scelta del tutto libera oppure imposta dalla necessità di evitare le conseguenze penali a cui il *relocator* incorrerebbe qualora facesse rientro nel Paesi d'origine o di cittadinanza. Inoltre, per un esame dei profili critici dell'inquadramento giuspenalistico del fenomeno dei *foreign fighters* negli ordinamenti nazionali, si rinvia a L. DELLA TORRE, *Tra guerra e terrorismo: le giurisprudenze nazionali alla prova dei foreign fighters*, in *Dir. Pen. Comp*., 2/2017, p. 170.

[259] Sul punto si veda il Considerando n. 6.

L'art. 5 della direttiva prevede il reato di "*Pubblica provocazione per commettere reati di terrorismo*".

Sotto il profilo oggettivo, la condotta consiste nella diffusione (o in ogni altra forma di pubblica divulgazione) - con qualsiasi mezzo - di un messaggio che promuova il compimento di reati di terrorismo, con il pericolo della commissione di uno o più di essi.

Il comportamento penalmente rilevante, per espressa previsione della norma, può essere realizzato anche in modalità *online*.

Trattasi di una previsione innovativa, dal momento che – diversamente dalle fattispecie italiane introdotte in materia - non ricorrono riferimenti agli «strumenti informatici» né agli «strumenti telematici», i quali, come si è visto nel precedente capitolo, sono elementi essenziali del fatto tipico dei cosiddetti *reati informatici*[260].

---

[260] La fattispecie di "*Addestramento ad attività con finalità di terrorismo internazionale*" (art. 270-*quinquies* c.p.) rappresenta il principale riferimento codicistico al cyberterrorismo prevede un aumento della pena «se il fatto di chi addestra o istruisce è commesso attravreso strumenti informatici». Per un esame della fattispecie si veda A. VALSECCHI, *Addestramento ad attività con finalità di terrorismo anche internazionale" (art. 270-quinquies c.p.): la prima pronuncia della cassazione,* nota a Cass. pen., Sez. VI, sent. 20.7.2011 (dep. 25.7.2011), n. 29670 - Pres. e Rel. De Roberto, in *Dir. Pen. Cont*., 20.12.2011. Ad ogni modo giova osservare che l'art. 24 della legge 20 novembre 2017, n. 167, recante "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea*" ha dato espressa attuazione all'art. 20 della direttiva 2017/541, il quale prescrive che gli Stati membri adottino le misure necessarie affinché le autorità competenti, da un lato, dispongano, in materia di terrorismo, di strumenti di indagine efficaci quali quelli usati contro la criminalità organizzata (par. 1) e, dall'altro lato, possano congelare o confiscare i proventi derivati dall'atto di commettere o di contribuire alla commissione di un reato terroristico. Diversamente, per quanto attiene alle altre disposizioni della direttiva in esame, il legislatore italiano ha ritenuto che la maggior parte degli obblighi scaturenti dalla direttiva sia già soddisfatta all'interno delle fattispecie penali previste dagli art. 270-*bis* c.p. e ss. Sul tema SANTINI, *L'Unione europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017*/541, op. cit., pp. 32-42, ove si evidenzia che la direttiva 2017/541 non ha richiesto «*molti interventi al nostro legislatore che, con il d.l. 7/2015 e la l. 153/2016, ha in buona parte anticipato il contenuto della presente direttiva sulla scia delle indicazioni già contenute nella risoluzione 2178(2014) del Consiglio di sicurezza delle Nazioni Unite e nel protocollo addizionale alla Convenzione del Consiglio d'Europa per la prevenzione del terrorismo del 22 ottobre 2015*». Infatti, secondo l'autore, i reati di terrorismo *ex* art. 3 della direttiva 2017/541 sono già ricompresi nella definizione di cui all'art. 270-*sexies* c.p. Le condotte di *direzione di un gruppo terroristico* o di *partecipazione alle attività di un gruppo terroristico* (art. 4 della direttiva) acquistano normalmente rilievo penale, nel nostro ordinamento, ai sensi

La scelta del legislatore europeo di introdurre il concetto di «condotte *online*», che non ha implicazioni meramente formali, deve essere letta come un chiaro riferimento alle condotte commesse nel cyberspazio e, quindi, ai *cybercrimes*[261].

---

dell'art. 270-*bis* c.p. Parimenti, le condotte di *pubblica provocazione per commettere reati di terrorismo* sono già sussumibili nell'ambito di applicazione dell'art. 414, co. 4, c.p., che punisce le condotte di chi, pubblicamente, istiga alla commissione di un delitto di terrorismo o ne fa apologia. Problemi di adeguamento non sorgono nemmeno con riferimento alla fattispecie di *finanziamento del terrorismo* (art. 11 della direttiva), già pienamente riconducibile alla fattispecie di cui all'art. 270-*quinquies.1* c.p. Per quanto riguarda gli altri reati connessi ad attività terroristiche *ex* art. 12 della direttiva (furto aggravato, estorsione, produzione o utilizzo di documenti falsi allo scopo di commettere un reato di terrorismo) essi sono già punibili nel nostro ordinamento per effetto del combinato disposto delle norme che puniscono furto, estorsione e produzione di documenti falsi e dell'aggravante *ex* art. 1 del d.l. 625/1979. L'autore, poi, si sofferma sulle condotte di *reclutamento a fini terroristici* (art. 6 della direttiva) e su quella di *viaggi a fini terroristici* (art. 9 della direttiva). Esse, che formalmente sono sussumibili entro le fattispecie previste dagli artt. 270-*quater* c.p. e 270-*quater.1* c.p., rispettivamente, impongono un adeguamento, ad oggi mancante, non soltanto interpretativo delle richiamate disposizioni codicistiche. Secondo Santini, infatti, i concetti di «arruolamento» e di «viaggio» sarebbero affetti da indeterminatezza, onde sarebbe indispensabile procedere ad una loro definizione nel senso indicato dal legislatore europeo nella direttiva 2017/541. In particolare, l'autore opinerebbe che l'art. 9 della direttiva, richiedendo agli Stati di punire il viaggio a fini terroristici, anticiperebbe sensibilmente la soglia della rilevanza penale rispetto alla corrispondente fattispecie italiana. L'art. 270-*quater.1* c.p., infatti, punisce gli *organizza, finanzia o propaganda* il viaggio finalizzato al compimento delle condotte terroristiche. Il mero viaggio, invece, resterebbe soggetto alle misure di prevenzione *ex* art. 4, lett. d), d.lgs. 159/2011 (senza poter essere sussunto entro un'autonoma fattispecie delittuosa).

[261] La più autorevole dottrina in materia si è dimostrata concorde nel ritenere che le condotte *online*, alle quali viene fatto riferimento nella direttiva (UE) 2017/541 e che – diversamente dalle condotte meramente informatiche – sono caratterizzate da strategie di comunicazione raffinate e multicanale, risultano particolarmente pericolose per la sicurezza della collettività, dal momento che la struttura della rete internet, per la sua vastità, non consente un controllo capillare efficace e, al contempo, è in grado di raggiungere i luoghi più disparati del pianeta, favorendo l'auto-addestramento anche di chi si trova lontano dai centri territoriali della rete terroristica. Cosi V. NARDI, *La punibilità dell'istigazione nel contrasto al terrorismo internazionale*, *op. cit*., p. 120; concordemente M. MAGGIONI, P. MAGRI, *Twitter e jihad. La comunicazione dell'Isis*, Epoké, 2015, pp. 92 e ss., in cui emerge come i gruppi terroristici abbiano elaborato nuove strategie di comunicazione (articolate su più livelli), secondo una diversificazione degli strumenti mediali in base ai vari obiettivi e ai destinatari di riferimento. A titolo esemplificativo si pensi che il sistema di propaganda adottato dal *Da'ish* contava quaranta media locali, cinque case di produzione e oltre cinquantamila account *Twitter*. Inoltre, cfr. A. LAVORGNA, *Cybercrimes*, op. cit., pp. 217-220, in cui l'autrice evidenzia che, a causa del recente sviluppo conosciuto dalle tecnologie cibernetiche e del loro sviluppo, oggigiorno è sempre più difficile distinguere la realtà *online* da quella *offline* con la conseguenza che «in many cases, cybercrimes are not confined to cyberspace but rather spill over into the physical space, expanding

Invero, la provocazione per commettere reati terroristici rappresenta un esempio emblematico di nuova condotta che può essere posta in essere attraverso i *social networks*, attesa l'efficacia dimostrata da questi ultimi in ordine alla diffusone e alla promozione di messaggi, anche indirettamente, specie tra gli utenti più giovani[262].

In ogni caso rileva osservare che, ai fini dell'integrazione della fattispecie in parola (come chiarito dall'art. 13 della direttiva), non è necessaria la commissione del reato terroristico (bastandone il mero pericolo), con conseguente sussumibilità nella stessa delle condotte che, ad esempio, si esauriscono nell'esaltazione sui *social networks* degli attentatori suicidi o nella diffusione di immagini di brutali assassinii posti in essere da un determinato gruppo terroristico[263].

Sotto il profilo soggettivo, invece, l'art. 5 richiede che il soggetto agente ponga in essere la condotta *intenzionalmente* e, quindi, animato dalla volontà di realizzare, con la sua azione od omissione, proprio l'evento tipizzato dalla fattispecie, ovverosia provocare alla commissione del reato terroristico.

La fattispecie di "*Pubblica provocazione per commettere reati di terrorismo*", come prevista dall'art. 5 della direttiva, comporta innegabilmente una limitazione della *libertà d'espressione* (artt. 10 CEDU[264] e 11 CDFUE[265]), la quale non include soltanto la libertà di opinione, bensì anche quella di ricevere o

---

criminal possibilities through technology». *Ibidem*, p. 180, ove si evidenzia che i gruppi terroristici fanno ormai sistematicamente utilizzo di *apps* e *social media* come *networks* commerciali generalisti, i *social networks* più diffusi e sinanco i *video games online*. In particolare, sin dal 2010, al-Qaeda ha pubblicato, nella penisola arabica "*Inspire*", ovverosia una rivista *online* in inglese, usata da tutti gli affiliati all'associazione per reperire istruzioni e tecniche per porre in essere attacchi terroristici.

[262] A. LAVORGNA, *Cybercrimes*, op. cit., p. 180, in cui si legge che: «Through online propaganda, terrorists can radicalise and recruit individuals – often very vulnerable young people, including a large number of young women and adolescent girls». In particolare, evidenzia l'autrice, tra le modalità più diffuse per propagandare l'ideologia terroristica figura il caricamento di video, capace di radicalizzare i più giovani e le persone con bassi livelli di istruzione.

[263] S. SANTINI, *L'Europa compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, op. cit., pp. 16-17.

[264] L'art. 10, par. 1, CEDU è rubricato "*Libertà di espressione*".

[265] L'art. 11 CDFUE e rubricato "*Libertà di espressione e d'informazione*".

di comunicare informazioni o idee, *senza ingerenza delle Autorità pubbliche* e *senza frontiere*.

Con particolare riferimento all'art. 10 CEDU, rileva evidenziare che il relativo par. 2 ammette che la libertà d'espressione possa essere sottoposta a formalità, condizioni, restrizioni o sanzioni, solo laddove esse siano necessarie alla *sicurezza nazionale*, all'*integrità territoriale* o alla *pubblica sicurezza*, alla *difesa dell'ordine* e alla *prevenzione dei reati*, alla *protezione della salute* o della *morale*, alla *protezione della reputazione o dei diritti altrui*, per *impedire la divulgazione di informazioni riservate* o per garantire l'*autorità e l'imparzialità del potere giudiziario*. Tuttavia si ritiene che le limitazioni al diritto d'espressione, come chiarito dal Considerando n. 40 della direttiva in esame[266], non possano riguardare anche le condotte di diffusione di opinioni che - pur riflettendo posizioni radicali, polemiche o controverse in merito a questioni politiche sensibili - non siano assistite dall'intento di provocare la commissione di un reato terroristico (sotto il profilo soggettivo) e non siano concretamente idonee a produrre il pericolo della stessa (sotto il profilo oggettivo).

La dottrina ha osservato come il diritto eurounitario, attraverso la fattispecie prevista dall'art. 5 della direttiva, abbia imposto agli Stati membri di punire tutte quelle condotte di cosiddetta «provocazione indiretta», suscettibili cioè di dare semplicemente luogo al rischio che possano essere commessi uno o più dei reati ivi indicati[267].

La direttiva del 2017, inoltre, prevede due fattispecie dedicate all'addestramento per il compimento di attività con finalità di terrorismo, ovverosia la "*Fornitura di addestramento a fini terroristici*" (*ex* art. 7) e la

---

[266] Considerando n. 40 della direttiva (UE) 2017/541: «La presente direttiva non dovrebbe in alcun modo essere interpretata come intesa a limitare od ostacolare la diffusione di informazioni a fini scientifici, accademici o di comunicazione. L'espressione nel dibattito pubblico di opinioni radicali, polemiche o controverse in merito a questioni politiche sensibili non rientra nell'ambito di applicazione della presente direttiva e, in particolare, della definizione di pubblica provocazione per commettere reati di terrorismo».

[267] V. NARDI, *La punibilità dell'istigazione nel contrasto al terrorismo internazionale*, op. cit., 1/2017, p. 123, in cui l'autrice definisce la fattispecie *ex* art. 5 come una forma di «provocazione indiretta», in contrapposizione alle forme di istigazione.

"*Ricezione di addestramento a fini terroristici*" (*ex* art. 8). Esse puniscono rispettivamente la condotta di chi impartisce e quella di chi riceve 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 alla commissione di uno o più reati terroristici[268].

Orbene, benché manchi un espresso riferimento alla possibilità di porre in essere le condotte relative ai predetti reati in modalità *online*, non vi è alcun dubbio che l'addestramento relativo alla fabbricazione di armi o di esplosivi o alle tecniche per commettere reati terroristici trovi nell'*Internet*, nei *social networks* e, più in generale, nel *cyberspace* dei potenti strumenti per mettere in comunicazione docente e discente[269].

In particolare, ai fini dell'integrazione del reato *di ricezione di addestramento a fini terroristici*, è necessario che l'addestrato ricopra un *ruolo attivo nella propria formazione*, con la conseguenza che il semplice fatto di visitare siti *web* contenenti informazioni o di ricevere passivamente comunicazioni che siano – solo astrattamente – rilevanti per l'addestramento non è sufficiente[270].

---

[268] Per un esame dettagliato delle fattispecie di addestramento si rinvia a S. SANTINI, *L'Unione europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, op. cit., pp. 21 e ss.

[269] L'utilità degli strumenti cibernetici, in relazione alle condotte di addestramento, è ancor più evidente qualora docente e discente si trovino a grande distanza oppure quando vi è la necessità di rendere più chiare delle spiegazioni riguardanti dispositivi il cui utilizzo richiede particolari conoscenze tecniche. Sulla prevenzione delle concotte *online* di addestramento si veda V. NARDI, *La punibilità dell'istigazione nel contrasto al terrorismo internazionale*, op. cit., p. 120, in particolare la nota 28. Sul punto è opportuno evidenziare che nella *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* (il riferimento è chiaramente alla direttiva 2017/541), disponibile al link *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52015PC0625&rid=4*, p. 17, emerge la necessità di prevenire le condotte di addestramento, peculiarmente di quelle poste in essere in modalità *online*, e precisamente di: «contrastare la diffusione di istruzioni e manuali (*online*) ai fini dell'addestramento e della pianificazione di attentati e più specificatamente la diffusione (attraverso Internet) di informazioni sulle risorse e sui metodi terroristici, che funge in tal modo da "*campo di addestramento virtuale*"».

[270] S. SANTINI, *L'Europa compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, op. cit., p. 22.

Menzione a parte merita l'*autoapprendimento*, ovverosia la condotta di chi si addestra da sé, reperendo autonomamente il materiale su cui formarsi e acquisendo conoscenze e particolari abilità pratiche. Ebbene, il Considerando n. 11 della direttiva sembrerebbe ammettere la riconducibilità dell'autoapprendimento entro il concetto di *ricezione di addestramento*, sempreché la prima condotta – posta in essere attraverso *Internet* o tramite la consultazione di altro materiale didattico *online* - derivi da un comportamento attivo, posto in essere con l'intento di commettere (o quantomeno di contribuire alla commissione di) un reato terroristico[271].

6.2. Il terrorismo online e la strategia europea per il suo contrasto preventivo: le misure della rimozione e del blocco (art. 21 della direttiva 2017/541)

La direttiva 2017/541 non si limita a tipizzare delle *fattispecie prevenzionistiche* contro le condotte di terrorismo poste in essere con tecnologie cibernetiche (ad esempio di *social networks*), ma indica delle *ulteriori misure* che gli Stati devono adottare per *prevenire* il fenomeno.

In particolare, l'art. 21 della direttiva fa riferimento alle misure per contrastare i contenuti diffusi *online* nel contesto della pubblica provocazione per commettere un reato di terrorismo.

---

[271] R. FLOR, *Cyber-criminality: le fonti internazionali ed europee*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, op. cit., p. 125; S. SANTINI, *L'Europa compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, op. cit., p. 22. Sul punto rileva osservare che il Considerando n. 11 fornisce all'interprete due criteri per valutare la sussistenza dell'atteggiamento psicologico descritto: il *tipo di materiale consultato* e la *frequenza della consultazione*. Il fatto di visitare siti *web* ovvero di raccogliere materiale per finalità legittime - tra le quali certamente rientrano gli scopi di tipo accademico o di ricerca - non può essere considerato un comportamento sussumibile entro la fattispecie *ex* art. 8 della direttiva. Sul punto, inoltre, A. LAVORGNA, *Cybercrimes*, op. cit., p. 180, ove, fermo l'esame delle fattispecie di cui agli artt. 5, 7 e 8 della direttiva (UE) 2017/541, l'autrice osserva che le più rivoluzionarie opportunità criminogene offerte dalla cibernetica ai terroristi consistono nel poter *propagandare le loro idee in Internet*, nel *creare un senso d'appartenenza ad una comunità di persone dotate della medesima impostazione mentale* e nel *predisporre una formazione ed addestramento per i sostenitori online*.

La principale misura in materia consiste nella tempestiva *rimozione*, alla fonte, dei contenuti che siano ospitati nel territorio dello Stato (art. 21, par. 1)[272]. Tuttavia, qualora la rimozione non fosse impossibile, l'art. 21, par. 2, consente agli Stati di *bloccare l'accesso* a tali contenuti agli utenti di *Internet* che si trovino sul loro territorio[273].

L'art. 22 della direttiva, invece, prescrive che - attesa la pervasività delle misure di rimozione e blocco succitate - gli Stati membri devono in ogni caso garantire agli utenti finali ed ai fornitori di servizi un adeguato livello di *certezza* e *prevedibilità del diritto*, nonché la possibilità di ricorrere per via giudiziaria, conformemente al diritto nazionale ed alla Carta dei diritti fondamentali dell'Unione europea. Tale previsione rappresenta una vera e propria clausola di salvezza, che, attesa la pervasività delle misure di prevenzione previste, mira a garantire il bilanciamento fra le esigenze securitarie legate al terrorismo e la necessità di garantire il rispetto dei diritti civili fondamentali, dei quali lo Stato democratico, dotato di una Costituzione antropocentrica, si fa portatore.

Sempre in tema di limitazione delle misure previste dalla direttiva, è interessante osservare come il Considerando n. 23 della stessa - nel precisare che la rimozione dei contenuti *online* (art. 5) non dovrebbe pregiudicare le disposizioni della direttiva 2000/31/CE (relativa a taluni aspetti giuridici dei

---

[272] Sul punto è opportuno osservare che l'art. 21, par. 1, della direttiva prevede altresì che gli Stati devono adoperarsi al fine di rimuovere i contenuti *online* riconducibili alla pubblica provocazione per commettere un reato di terrorismo anche quando essi siano ospitati al di fuori del loro territorio, cooperando con i Paesi terzi direttamente interessati. Per un inquadramento della disposizione in parola, si veda L. MARINI, *L'evoluzione della disciplina internazionale in materia di terrorismo: qualche spunto recente fra Onu ed Europa*, in *QuestioneGiustizia*, disponibile al link: *https : / / www . questionegiustizia . it / rivista / articolo / l – evoluzione - della-disciplina - internazionale – in – materia – di - terrorismo_qualche – spunto – recente - fra – onu – ed – europa _ 452 . php,* in cui l'autore precisa che il contenuto dell'art. 21 della direttiva si colloca in linea con le risoluzioni dell'Assemblea generale dell'ONU nn. 60/288 e 70/291 - entrambe dedicate alle misure per la lotta al terrorismo internazionale – e, anzi, può essere meglio interpretato alla luce dei Consideranda della stessa direttiva nn. 31, 32 e 33 (per quanto concerne i temi generali legati alla radicalizzazione) e 10 (relativo alla criminalizzazione delle condotte).

[273] L'art. 21, par. 3 della direttiva, al fine di ricercare il bilanciamento tra le esigenze di sicurezza, da un lato, e la libertà di manifestare il proprio pensiero, dall'altro, prescrive che, in ogni caso, le misure di rimozione e blocco devono essere stabilite secondo procedure trasparenti ed essere limitate allo stretto necessario.

servizi della società dell'informazione, in particolare il commercio elettronico) - *esclude che i fornitori di servizi di hosting possano essere destinatari di obblighi di sorveglianza* rispetto alle informazioni che trasmettono (o memorizzano) o *di ricerca* rispetto a fatti che indichino la presenza di attività illecite. Conseguentemente la responsabilità penale degli *internet service providers* non sarebbe ravvisabile in relazione alle condotte terroristiche *online* poste in essere da terzi, che interessino i servizi erogati, sempreché i fornitori non siano a conoscenza dell'illiceità delle condotte (o delle informazioni che ne sono oggetto) né dei fatti o delle circostanze che rendono manifesta tale illiceità[274].

---

[274] La responsabilità penale degli *Internet Service Providers* (ISP) e, più in generale, dei fornitori dei servizi di *hosting* per le pubblicazioni effettuate da terzi sugli spazi virtuali messi a disposizione dai primi è una questione assai delicata e tuttora dibattuta. La giurisprudenza, infatti, ha espresso orientamenti ondivaghi nel corso del tempo. Con la sentenza del 17.12.2013, n. 5107, la terza Sezione della Cassazione, conformemente a quanto sarebbe stato previsto più tardi nel Considerando n. 23 della direttiva 2017/541, ha escluso la responsabilità penale del fornitore di servizi di *hosting* per le pubblicazioni di terzi a norma dell'art. 40, co. 2, c.p., attesa la mancanza di una *posizione di garanzia* e di obblighi di sorveglianza in capo agli *Internet Service Providers*, giacché nessuna disposizione «*prevede che vi sia in capo al provider, sia esso anche un hosting provider, un obbligo generale di sorveglianza dei dati immessi da terzi sul sito da lui gestito*». Diversamente, secondo la Cassazione, sarebbe possibile ravvisare una responsabilità penale dell'*Internet Service Provider*, qualora esso, dopo la pubblicazione dei contenuti illeciti da parte dei soggetti terzi, non si attivi per rimuoverli, sempreché sia a conoscenza della loro illiceità penale. Tuttavia, anche nel caso da ultimo descritto, la giurisprudenza esclude una contestazione per concorso omissivo *ex* art. 40, co. 2, c.p. (essendosi il reato ormai realizzato) in capo all'ISP, al quale, tuttalpiù, potrebbero contestarsi fattispecie commissive autonome da individuarsi caso per caso. Conformemente, in dottrina, D. COSTA, *La responsabilità dell'Internet Service Provider per i reati in materia di diritto* d'autore, in *Giur. Pen*., 2/2022, pp. 47-51, ove l'autore, con riferimento alla responsabilità omissiva dell'*ISP*, precisa che: «[…] *l'ordinamento italiano pare adottare come postulato l'esclusione tout court dell'attribuzione all'ISP di un ruolo di "controllore" rispetto alle condotte illecite aventi luogo nel ciberspazio, in relazione alle quali l'intero panorama legislativo interno continua a negare, in capo al provider, posizioni di garanzia ovvero obblighi di sorveglianza. La linea adottata dal legislatore risulta peraltro condivisa, ad oggi, anche dalla giurisprudenza prevalente* […]». Diversamente l'autore ritiene più agevole la responsabilizzazione dell'ISP come concorrente attivo nel reato commesso dagli utenti, precisando che: «*i pochi dubbi sull'ammissibilità del concorso materiale nei reati sono stati definitivamente dissipati dall'art. 102-septies L. Aut., introdotto dal D.Lgs. 177/2021, che esclude ogni limitazione di responsabilità per il provider che agevoli condotte aventi ad oggetto l'illecita condivisione di opere dell'ingegno in rete*». Ad ogni modo, si segnala che la Cassazione è tornata a pronunciarsi sul tema con sentenza 27.12.2016, n. 59496 della Sezione Quinta, che ha ritenuto responsabile *ex* art. 40, co. 2, c.p. un ISP che aveva omesso di rimuovere un contenuto diffamatorio pubblicato sulla *community* del sito da lui gestito. Nella loro argomentazione i giudici hanno ritenuto

La direttiva 2017/541 propone un approccio per il contrasto del terrorismo *online*, che, nel complesso, è fondato sulla prevenzione della radicalizzazione e del reclutamento nelle file del terrorismo. Invero, come si legge nel Considerando n. 31 della direttiva, tale approccio deve essere «a lungo termine, proattivo e globale» e deve combinare misure di giustizia penale con adeguate politiche nei settori dell'istruzione, dell'inclusione sociale e dell'integrazione, nonché con l'offerta di programmi efficaci di deradicalizzazione. L'adozione di misure di prevenzione, che vedono il coinvolgimento di così tanti settori unitamente a quello del diritto penale, non può prescindere da un consolidato meccanismo che consenta lo scambio di informazioni in tempi celeri e senza ostacoli burocratici, nonché dall'impegno di professionisti ed esperti appartenenti alla società civile, secondo lo schema della *positive prevention* (e specialmente della *social prevention*), già diffuso nei Pasi di *common law* e di cui si dirà nel successivo Capito III[275].

Alla luce dell'esame delle misure di prevenzione previste dalla direttiva 2017/541, è evidente come essa si collochi perfettamente nel solco della cosiddetta *Strategia antiterrorismo dell'Unione europea* descritta dal Consiglio europeo nel documento 14469/4/05 del 30.11.2005, volta al contrasto preventivo della radicalizzazione e del reclutamento nelle file del terrorismo, rappresentandone anzi un aggiornamento alla luce delle novità cibernetiche[276].

---

sussistere l'obbligo di impedire non tanto il reato a monte, quanto il protrarsi dei suoi effetti. Altra dottrina, invece, pare ammettere la configurabilità, in capo all'*hosting provider*, di un'ipotesi di responsabilità omissiva impropria, ai sensi dell'art. 40, co. 2, c.p., «qualora, essendo a conoscenza dell'attività illecita già perpetrata, esso non impedisca la relativa diffusione telematica, con l'effetto che l'omissione rappresenta la partecipazione concorrente alla consumazione delittuosa». Così G. STEA, *La responsabilità penale dell'internet provider*, nota a Cass. Pen., Sez. V, sent. 1.3.2016 (ud. 13.7.2015), n. 8328, in *Giur. Pen*., 11/2016, pp. 4 e ss.

[275] Con riguardo alla predisposizione delle misure di formazione e sensibilizzazione in questione, il Considerando n. 33 della direttiva evidenzia l'importanza di favorire la cooperazione fra i professionisti della società civile, da un lato, e le società private, le comunità locali e gli altri soggetti interessati, dall'altro.

[276] *The European Union Counter - Terrorism Strategy*, Council of the EU doc. 14469/4/05, 30.11.2005, disponibile al link *https : / / data . consilium . europa . eu / doc / document / ST % 2014469 % 202005 % 20REV % 204 / IT / pdf*.

Il rafforzamento della risposta di giustizia penale in chiave preventiva contro i terroristi si è reso necessario per lo sviluppo, da parte degli stessi, della capacità di tradurre idee in azioni, affinatasi a partire da inizio millennio grazie ad Internet e al *cyberspace*, che hanno reso più agevole l'accesso ai contenuti radicali ed all'addestramento[277]. In particolare, il Consiglio europeo evidenzia come le associazioni terroristiche abbiano fatto massicciamente ricorso allo strumento della propaganda *online*, al fine di distorcere la verità sui conflitti nel mondo e giustificare l'impegno contro gli obbiettivi presi di mira[278].

In accordo alla *Strategia* del 2005, «*prevenire*» significa intervenire per impedire le affiliazioni al terrorismo, affrontando i fattori e le cause profonde che possono portare alla radicalizzazione ed al reclutamento. Per questa ragione il Consiglio ritiene necessario individuare e contrastare i *modi*, la *propaganda* e le *condizioni* attraverso i quali le persone possono essere attratte dal terrorismo.

Conclusivamente rileva osservare che, secondo la *Strategia* europea, i fattori che contribuiscono alla creazione dell'ambiente favorevole alla radicalizzazione (e, quindi, al «*contesto*» delle condotte terroristiche *ex* art. 270-*sexies* c.p.) sono: *uno Stato dotato di una Personalità debole* o, all'estremo opposto, *autocratica*[279]; *una modernizzazione rapida ma giuridicamente*

---

[277] Ivi, p. 8, il punto n. 9.

[278] Ivi, p. 8, il punto n. 10.

[279] Ivi, p. 9, il punto n. 11, in cui, ad essere precisi, si legge che il primo fattore, nella traduzione italiana, consiste in un «governo carente o autocratico» («poor or autocratic governance» nella versione inglese). Ad ogni modo rileva osservare che tra i principali indici sintomatici della debolezza della Personalità dello Stato figura certamente il cattivo esercizio del potere legislativo, che, in ultima analisi, si manifesta nell'incapacità del legislatore nazionale di disciplinare normativamente una determinata materia – e, con particolare riferimento al diritto penale, l'incapacità di contrastare un determinato fenomeno criminoso – o, comunque, nel disciplinarla in modo inadeguato o, peggio, in violazione dei principi costituzionali e democratici. Orbene, sulla scorta di queste considerazioni, è indubbio che il nostro ordinamento nazionale abbia dato prova di debolezza rispetto al cyberterrorismo. Per un esame del difficile rapporto fra democrazia e *cyberspace*, rispetto al quale la prima – così come tradizionalmente intesa – sarebbe addirittura incompatibile, si rinvia a M. WEBB (foreword by C. DOCTOROW), *Coding Democracy. How hackers are dsrupting power, surveillance and authoritarianism*, op. cit., pp. 105-108. Tra le principali argomentazioni addotte dall'autore figura quella secondo cui: «democracy traditionally has been based on the nation State, and in maps of the digitally networked world, the nation state is looking increasingly irrelevant».

incontrollata, come quella che si sta registrando in relazione alla rivoluzione cibernetica; l'*assenza di prospettive politiche ed economiche, nonché di opportunità di istruzione*[280]. Ebbene, come si è detto, non v'è chi non veda come i tre fattori appena riferiti coesistono tutti nel presente periodo storico di crisi[281], ricreando dunque la combinazione idealtipica per lo sviluppo del cyberterrorismo.

6.3. Il regolamento (UE) 2021/784 per il contrasto della diffusione dei contenuti terroristici online e dell'uso dei servizi di hosting a fini terroristici

Il Regolamento (UE) 2021/784 del 29 aprile 2021 è dedicato al contrasto, *in chiave preventiva*, della diffusione dei contenuti *online* e dell'uso dei servizi di *hosting* per fini terroristici. Esso prescrive che gli Stati integrino le normative nazionali in materia con strategie che prevedano il rafforzamento dell'*alfabetizzazione digitale* e del «*pensiero critico*», lo sviluppo di «*narrazioni alternative* e di *controargomentazioni*», le iniziative di «*dialogo con le comunità interessate*», al fine di prevenire ogni forma di radicalizzazione terroristica[282].

Dette misure confermano la preferenza accordata dal diritto eurounitario all'approccio *multisettoriale* e *multilivello* per prevenire il fenomeno terroristico *online*, combinando tra loro «misure legislative», «misure non legislative» e

---

[280] Ivi, p. 9, il punto n. 11, in cui si precisa che il terzo fattore, ovverosia l'*assenza di prospettive politiche ed economiche* ed *opportunità di istruzione*, potrebbe interessare anche solo determinate fasce della popolazione.

[281] P. MORO, *Il diritto come processo. Principi, regole e brocardi per la formazione del giurista*, op. cit., pp. 10-11.

[282] Sul punto si veda il Considerando n. 2 del regolamento 2021/784. Del concetto di «alfabetizzazione informatica» (oltre che di quello di «igiene informatica»), come si è detto, viene fatta menzione anche nell'art. 10, lett. b) del regolamento (UE) 2019/881. Tale concetto fa riferimento alla necessità che gli Stati predispongano delle misure volte a fornire una formazione in materia di cibernetica e di utilizzo delle tecnologie dell'informazione a tutti gli utenti del *cyberspace*, in un'ottica preventiva rispetto ai *cybercrimes*. Tale formazione si rivela indispensabile con riguardo ai contenuti *online*, al fine di assicurare un corretto utilizzo delle piattaforme di comunicazione (in particolare dei *social networks*) e, quindi, di agevolare il riconoscimento del carattere terroristico dei contenuti ivi pubblicati.

«misure volontarie»[283] basate sulla collaborazione tra le Autorità pubbliche ed i prestatori di servizi di *hosting*, in ogni caso nel pieno rispetto dei diritti fondamentali[284].

A norma dell'art. 2, n. 1 del regolamento, per «prestatore di servizi di *hosting*» (*hosting service providers*) si intende il soggetto che svolge qualsiasi servizio della società dell'informazione, normalmente dietro retribuzione, a distanza, per via elettronica e, in ogni caso, volto a memorizzare le informazioni provenienti da un fornitore di contenuti (art. 2, n. 2)[285]. Tra i principali *hosting service providers* figurano i fornitori di *servizi di social media*, di *condivisione di video, audio e immagini*, nonché i fornitori di *servizi di condivisione di file e altri servizi cloud* (Considerando n. 14).

L'art. 2, n. 7, invece, fornisce la definizione di «*contenuti terroristici*», i quali possono consistere in materiali che alternativamente: istigano alla commissione di uno dei reati *ex* art. 3, par. 1, lett. da a) a i), della direttiva 2017/541[286]; sollecitano una persona o un gruppo di persone a commettere (o a contribuire a commettere) uno dei reati *ex* art. 3, par. 1, lett. da a) a i), della direttiva 2017/541; sollecitano una persona o un gruppo di persone a partecipare alle attività di un gruppo terroristico *ex* art. 4, lett. b), della direttiva 2017/541; impartiscono istruzioni per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose, ovvero altri metodi o tecniche specifici, allo scopo di commettere (o di contribuire alla commissione di) uno dei reati di terrorismo *ex* art. 3, par. 1, lett. da a) a i), della direttiva 2017/541; costituiscono

---

[283]Considerando n. 3 del regolamento (UE) 2021/784.

[284]Tra i diritti fondamentali che, per espressa previsione del Considerando n. 10 del regolamento, devono essere in ogni caso rispettati nell'attuazione dell'approccio multisettoriale dell'Unione figurano: il *diritto al rispetto della vita privata*, il *diritto alla protezione dei dati personali*, il *diritto alla libertà di espressione* (compresa la *libertà di ricevere e comunicare informazioni*), la *libertà d'impresa*, nonché il *diritto ad una tutela giurisdizionale effettiva*.

[285] Sul punto rileva osservare che la diffusione dei contenuti sottende la loro *messa a disposizione* a favore di un numero potenzialmente illimitato di persone (art. 2, n. 3).

[286] La disposizione in parola precisa che tali materiali - direttamente o indirettamente (ad esempio mediante l'apologia di atti terroristici) – devono incitare a compiere reati di terrorismo, generando in tal modo il pericolo che uno o più di tali reati siano commessi.

una minaccia di commissione di uno dei reati *ex* art. 3, par. 1, lett. da a) a i), della direttiva 2017/541.

Ebbene, giova osservare come i predetti contenuti terroristici siano riconducibili ai reati di *pubblica provocazione* e di *addestramento a commettere un reato terroristico* - precedentemente esaminati - a conferma del fatto che per la loro integrazione, nella maggior parte dei casi, rileveranno «condotte *online*»[287].

Invero gli attacchi terroristici compiuti negli ultimi anni in Europa hanno dimostrato le accresciute abilità dei terroristi nell'uso della rete e di *Internet* per addestrare, reclutare, propagandare, intimorire la popolazione ed organizzare nuovi attentati. I contenuti diffusi, oltre che impattare significativamente sugli individui e sulla sicurezza, minano la fiducia riposta dagli utenti nelle piattaforme *online* e più in generale nelle tecnologie cibernetiche[288].

Attesi gli effetti descritti dall'art. 2, n. 7, il regolamento 2021/784 indica i parametri che i *prestatori di servizi di hosting* devono impiegare per valutare la natura terroristica dei contenuti pubblicati e, quindi, procedere alla loro rimozione (v. Considerando n. 11).

Detti parametri consistono nella «*natura*» e nella «*formulazione*» dei contenuti, nel «*contesto*» in cui sono diffusi e nel loro «*potenziale* di portare a conseguenze dannose, compromettendo la sicurezza e l'incolumità delle

---

[287] Per comprendere ed ampliare la definizione di «contenuto terroristico» è opportuno fare riferimento al Considerando n. 11 del regolamento, ove si prevede che, nella definizione di contenuto terroristico, debbano essere ricompresi: il materiale che fornisce indicazioni per la fabbricazione e l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose, nonché sostanze chimiche, biologiche, radiologiche e nucleari (CBRN), ovvero altri specifici metodi o tecniche, compresa la selezione degli obiettivi, al fine di commettere o contribuire alla commissione di reati di terrorismo. La disposizione in parola equipara ai suddetti materiali le immagini, le registrazioni audio e video, nonché le trasmissioni in diretta di reati di terrorismo, che generano il rischio della commissione di questi ultimi.

[288] M. MARTORANA, *Terrorismo sul web e contenuti online: il nuovo regolamento UE*, in *Altalex*, 25.5.2021, disponibile al link: *https : / / www . altalex . com / documents / news / 2021 / 05 / 25 / terrorismo - web - contenuti - online - nuovo - regolamento - europeo*, in cui l'autore evidenzia che i terroristi si sono recentemente dimostrati in grado di utilizzare in modo improprio non solo le più grandi piattaforme di *social media*, ma anche i servizi offerti dai più piccoli *hosting providers*.

persone»[289]. A parere di chi scrive, il concreto accertamento del carattere terroristico dei contenuti *online* è indispensabile al fine di evitare violazioni del principio di offensività, che si configurerebbero qualora la valutazione circa la natura illecita delle pubblicazioni (e la conseguente applicazione di misure restrittive della libertà degli autori) fosse devoluta ad automatismi fondati su algoritmi, incapaci di discernere il sarcasmo dalla fede, le notizie dalla propaganda o l'educazione dall'indottrinamento[290].

Il regolamento, oltre ad indicare i parametri da impiegare nella valutazione della natura terroristica dei contenuti pubblicati, prevede gli strumenti che gli Stati membri devono impiegare per la loro eliminazione[291].

---

[289] Il Considerando n. 11 del regolamento 2021/784 aggiunge che i fornitori dei servizi di *hosting* possano valutare la natura terroristica dei contenuti *online* alla luce di un ulteriore parametro, ovverosia l'inclusione del soggetto che ha prodotto o diffuso il contenuto (o al quale questo è comunque attribuibile) nell'apposito elenco delle persone, dei gruppi e delle entità coinvolti in atti terroristici (trattasi dunque di un criterio formale). Per un recente esame delle condizioni che giustificano la permeanza di un gruppo nel predetto elenco, si veda CGUE, Grande Sezione, sent. 23 novembre 2021, C-833/19 P e Trib. UE, sent. 4 settembre 2019, Hamas/Consiglio, T-308/18.

[290] Il riferimento alla *natura* e al *conteso*, come si è detto, consente di valutare la concreta idoneità offensiva delle condotte terroristiche come previsto dall'art. 1 della decisione-quadro 2002/475/GAI. Sul punto M. MARTORANA, *Terrorismo sul web e contenuti online: il nuovo regolamento UE*, op. cit.

[291] Sul sistema di misure predisposto dal regolamento (UE) 2021/784 per contrastare in via preventiva la diffusione di contenuti terroristici *online* si veda R. PEZZUTO, *Contenuti terroristici on line: l'unione europea lavora a nuove norme per prevenirne la diffusione*, in *Dir. Pen. Comp.*, op. cit., p. 41, in cui l'autore evidenzia che tale sistema supera il regime di «cooperazione volontaria tra gli Stati membri e l'industria digitale avviato dall'Unione nel 2015». Invero l'autore ritiene che tale regime di cooperazione si sia rivelato «non pienamente soddisfacente», onde doversi preferire l'adozione di «misure più rigorose di prevenzione e contrasto, fondate sull'imposizione di precisi obblighi giuridici a carico dei prestatori di servizi di *hosting*, che sono peraltro chiamati a collaborare tra loro e con le autorità competenti, compresa Europol, per mettere in atto più incisive misure proattive e migliori meccanismi di monitoraggio e risposta alle segnalazioni di contenuti illegali». Nello stesso senso anche M. MARTORANA, *Terrorismo sul web e contenuti online: il nuovo regolamento UE*, op. cit., in cui l'autore evidenzia che, sebbene sia indubbio che la cooperazione tra attori privati e pubblici abbia permesso di migliorare il contrasto alla diffusione dei contenuti terroristici *online*, essa non ha però completamente risolto il problema. Tra le cause principali di questo risultato insoddisfacente figurerebbe il «carattere volontario di questa forma di cooperazione tra i settori pubblico e privato, da cui è disceso il numero complessivamente ridotto dei prestatori di servizi coinvolti nella collaborazione, nonché la lentezza e la parzialità del processo di rimozione dei contenuti illeciti in parola».

Trattasi dei cosiddetti «*ordini di rimozione*» (art. 3), con i quali l'Autorità competente designata dallo Stato (art. 12)[292], al ricorrere di *casi di emergenza debitamente giustificati*, impone ai prestatori di servizi - direttamente e senza preavviso - di *rimuovere* i contenuti terroristici o di *disabilitare* l'accesso agli stessi in tutti gli Stati membri (art. 3, par. 1).

Tra i requisiti che, a norma dell'art. 3, par. 4 del regolamento, deve presentare l'*ordine di rimozione* figurano: a) i dati identificativi dell'autorità competente che emette l'ordine di rimozione (con firma, data e ora dell'emissione); b) la motivazione, sufficientemente dettagliata, per cui i contenuti sono considerati terroristici (con riferimento al tipo di materiale *ex* art. 2, n. 7); c) un indirizzo URL che consenta di individuare i contenuti terroristici; d) un riferimento al regolamento come base giuridica dell'ordine di rimozione; f) delle informazioni facilmente comprensibili sui mezzi per presentare ricorso contro l'ordine di rimozione da parte del prestatore di servizi di *hosting* e del fornitore di contenuti.

In ogni caso, giova evidenziare che, in mancanza del presupposto dell'*emergenza*, l'Autorità competente è tenuta ad informare il prestatore di servizi di *hosting* con un anticipo di almeno *dodici ore* rispetto all'emissione dell'ordine di rimozione, indicando dettagliatamente le procedure da seguire per adempiervi (art. 3, par. 2).

Il termine entro il quale i prestatori di servizi di *hosting* sono tenuti ad adempiere alla misura è piuttosto stringente, atteso che la *rimozione* o la *disabilitazione* deve avvenire «il prima possibile e in ogni caso entro un'ora dal ricevimento dell'ordine di rimozione» (art. 3, par. 3).

Questione più complessa, invece, è quella degli «*ordini di rimozione transfrontalieri*», i quali hanno come destinatari i fornitori di servizi di *hosting*

---

[292] Ogni Stato membro, a norma dell'art. 12, par. 1, è tenuto a designare delle Autorità competenti per: a) emettere ordini di rimozione a norma dell'art. 3; b) esaminare ordini di rimozione a norma dell'art. 4; c) sorvegliare l'attuazione delle misure specifiche a norma dell'art. 5; d) irrogare sanzioni a norma dell'art. 18. Gli Stati sono tenuti ad assicurare che le Autorità dispongano dei poteri necessari e delle risorse sufficienti per conseguire gli obiettivi e adempiere gli obblighi loro incombenti a norma del regolamento (art. 13, par. 1).

con sede principale (o legale rappresentante) in Stato diverso da quello al quale appartiene l'Autorità che emette l'ordine (art. 4, par. 1).

In questi casi l'art. 4, par. 1 del regolamento prevede che l'Autorità emittente trasmetta copia dell'ordine all'Autorità omologa dello Stato membro in cui il destinatario ha la sede principale (o il rappresentante legale). L'Autorità ricevente, di propria iniziativa, può esaminare l'ordine di rimozione per stabilire se esso violi in modo grave o manifesto il regolamento 2021/784 o la Carta dei diritti fondamentali dell'Unione europea e, in caso positivo, rifiutarne l'esecuzione[293].

L'art. 5 del regolamento prevede che i prestatori di servizi di *hosting* si dotino di ulteriori strumenti per prevenire la commissione dei reati terroristici che possono conseguire alla pubblicazione dei contenuti *online*[294]. In particolare l'art. 5, par. 2 prevede delle *misure specifiche* - la cui scelta spetta agli stessi prestatori - tra le quali figurano: a) adeguate misure o capacità tecniche e operative, quali personale o mezzi tecnici adeguati per individuare e rimuovere rapidamente o disabilitare l'accesso a contenuti terroristici; b) meccanismi facilmente accessibili e di facile uso per consentire agli utilizzatori di segnalare o indicare al prestatore di servizi di *hosting* presunti contenuti terroristici; c) qualsiasi altro meccanismo per sensibilizzare maggiormente in merito ai contenuti terroristici, quali i meccanismi di moderazione per l'utilizzatore; d) qualsiasi altra misura che il prestatore di servizi di *hosting* ritenga appropriata per contrastare la disponibilità di contenuti terroristici nei suoi servizi[295].

---

[293] L'art. 4, par. 3 prescrive un termine di 72 ore sia per l'esame della conformità dell'ordine di rimozione al regolamento 2021/784 (termine decorrente dalla ricezione della copia) sia per l'adozione di una decisione motivata sul tema.

[294] Le *misure specifiche* previste dall'art. 5 devono essere adottate dai prestatori di servizi in modo diligente, proporzionato e non discriminatorio, tenendo conto dei diritti fondamentali degli utilizzatori e dell'importanza che riveste la libertà d'espressione e d'informazione in una società aperta e democratica (art. 5, par. 1).

[295] In ogni caso le *misure specifiche* devono soddisfare tutti i requisiti previsti dall'art. 5, par. 3: a) devono essere efficaci per mitigare il livello di esposizione ai contenuti terroristici dei servizi di un prestatore di servizi di *hosting*; b) devono essere mirate e proporzionate, tenuto conto, in particolare, della gravità del livello di esposizione di un prestatore di servizi di *hosting* a contenuti terroristici, nonché delle capacità tecniche e operative, della solidità finanziaria, del

Dall'esame delle misure previste dal regolamento 2021/784, emerge come la più recente strategia europea per il contrasto dei reati di terrorismo si fondi sull'impiego di misure di prevenzione (anziché di repressione), le quali, intervenendo *ante delictum*, sono volte ad impedire la commissione degli stessi, incidendo direttamente sui contenuti terroristici *online* che possono esserne causa.

Le misure che il legislatore europeo prescrive per i fornitori di servizi cibernetici (compresi i *social networks*) possono avere natura negativa o preventiva. Nel primo gruppo figurano l'ordine di rimozione (anche transfrontaliero) e la disabilitazione dell'accesso ai contenuti (art. 3). Nel secondo gruppo, invece, rientrano delle misure specifiche che possono ricondursi entro due principali categorie: le *best practices* (quali, ad esempio, capacità tecniche, mezzi tecnici adeguati, meccanismi di segnalazione di contenuti sospetti ex art. 5, par. 2, lettere a e b) e l'*alfabetizzazione cibernetica* (sensibilizzazione in merito ai contenuti terroristici con meccanismi di moderazione *ex* art. 5, par. 2, lett. c).

7. Osservazioni conclusive

Il diritto dell'Unione europea disciplina in modo piuttosto dettagliato sia la materia dei *cybercrimes* sia quella dei reati di *terrorismo*, adottando per entrambe un approccio marcatamente preventivo. Tuttavia solo recentemente il legislatore europeo ha ravvisato l'opportunità di normare, sotto il profilo penale, anche il fenomeno frutto della commistione fra cibernetica e terrorismo, ovverosia il cyberterrorismo, pur senza mai esplicitare tale concetto[296].

---

numero di utilizzatori del prestatore di servizi di *hosting* e della quantità di contenuti forniti; c) devono essere applicate in una maniera che tenga pienamente conto dei diritti e degli interessi legittimi degli utilizzatori, in particolare dei diritti fondamentali degli utilizzatori, relativi alla libertà di espressione e di informazione, al rispetto della vita privata e alla protezione dei dati personali.

[296] C. LAMBERTI, *Gli strumenti di contrasto al terrorismo ed al cyber-terrorismo nel contesto europeo*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. VIII, n. 2, 5-8/2014, pp. 142 e ss.

Invero, allo stato, le condotte cyberterroristiche rilevano in relazione ad alcune fattispecie previste dalla direttiva 2017/541[297] - nella quale, tra l'altro, viene introdotto il concetto di «condotte *online*» - nonché alle definizioni e alle misure previste dal regolamento 2021/784[298], dedicato alla prevenzione della diffusione dei contenuti terroristici *online*.

A conferma della sostanziale autonomia concettuale raggiunta dal cyberterrorismo deve essere letto anche il riconoscimento, a livello europeo, di *nuovi interessi giuridici* da tutelare penalmente, i quali devono ricondursi ad *unum* entro il bene giuridico della cybersicurezza.

Il rafforzamento della tutela penale del nuovo bene giuridico postula, come emerso dallo fonti eurounitarie in materia, lo sviluppo della cyberresilienza, di adeguate misure volte alla prevenzione del terrorismo cibernetico e di un cyberspazio globale e aperto[299].

In particolare, dall'esame della direttiva 2008/114/CE, relativa alle infrastrutture critiche, è emerso che se, da un lato, è accoglibile la tesi secondo cui il *cyberspace* e le infrastrutture telematiche rientrano a pieno titolo nella definizione prevista dall'art. 2, lett. a) della direttiva predetta, dall'altro lato, è innegabile che tali infrastrutture, proprio per il loro carattere cibernetico, impongono di compiere alcune ulteriori riflessioni[300].

Infatti la cibernetica influisce sulle infrastrutture critiche aumentandone il grado di interconnessione a livello transnazionale. Tuttavia tale peculiarità, pur presentando innegabili aspetti favorevoli, contribuisce a rendere le infrastrutture eccezionalmente vulnerabili. Ogni connessione rappresenta un punto debole maggiormente esposto agli attacchi cibernetici e cyberterroristici, senza contare

---

[297] Il riferimento è alla *"Pubblica provocazione a commettere reati terroristici"* (art. 5), alla "*Fornitura di addestramento*" (art. 7) e alla "*Ricezione di addestramento*" (art. 8).

[298] Il riferimento è alla definizione di «*contenuti terroristici*» (art. 2, n. 7) e agli «*ordini di rimozione* » (art. 3).

[299] R. BRIGHI, P. G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea,* op. cit., p. 32.

[300] M. PASTORELLO, *How cyberspace is used by terrorist organization: possible threats to critical infrastructures? The most recent activities of cyber counterterrorism,* op. cit., pp. 117 e ss.

che l'interconnessione telematica - che supera i confini fisici degli Stati - rende possibile la propagazione delle conseguenze delle condotte criminose (originariamente indirizzate verso le strutture di un particolare Stato) secondo un meccanismo "ad effetto domino", tale da coinvolgere un numero potenzialmente infinto di sistemi tra loro collegati[301].

Per tutte queste ragioni sembra potersi affermare che le *infrastrutture critiche telematiche dello Stato* richiedono una particolare - e se possibile accresciuta - tutela rispetto alle altre infrastrutture, rendendosi necessario, a distanza di oltre un decennio dall'entrata in vigore della direttiva 2008/114/CE, aggiornare le definizioni previste dal relativo art. 2 ed aumentare gli *standards* minimi di tutela che gli Stati membri sono oggi chiamati a garantire, adeguandoli alle novità della cibernetica[302].

L'esame della direttiva 2013/40/UE (che ha sostituito la decisione-quadro 2005/222/GAI), poi, ha permesso di osservare come un *sistema di informazione* - al di là della definizione fornita dell'art. 2, lett. a) della stessa - sia costituito da due componenti. La prima di queste consiste nell'*hardware* e più in generale in tutti i *devices* che svolgono un trattamento di dati. La seconda, invece, consiste nei *dati stessi*. Ebbene, tale duplice natura richiama la definizione tripartita di *cyberspace* teorizzata da Even e Siman-Tov, dal momento che nel sistema di informazione è possibile ritrovare le componenti del *physical layer* (*hardware* e *devices*) e del *logical layer* (dati e informazioni). Invero tale accostamento non deve sorprendere, dal momento che anche il *cyberspace*, alla luce di tutte le considerazioni svolte nei precedenti capitoli, può essere inteso alla stregua di uno

---

[301] L. EDWARDS, B. SCHAFER, E. HARINJA, *Future Law, Emerging technology, regulation and ethics*, op. cit., p. 152-153, in cui si evidenzia che «the use of computing devices reliant upon increasingly complex software in our everyday lives has expanded hugely over the past decade, as demonstrated through the now ubiquitous 'smartphone' and tablets […]» e che negli ultimi anni si sia registrata una «increasing dependence on connectivity for the normal functioning of society» e, conseguentemente, un rapido aumento del rischio cibernetico.

[302] Sul punto è opportuno segnalare la recente *Proposta per una direttiva sulla resilienza delle Entità Critiche* (COM(2020) 829 final.) della Commissione europea (disponibile al seguente link: *https : / / eur – lex . europa . eu /legal – content / IT / TXT / PDF / ?uri = CELEX : 52020PC0829&from = IT*), che dovrebbe sostituire la direttiva 2008/114/UE.

sconfinato sistema di informazione - dotato dell'ulteriore componente dello *human layer* – che dunque deve essere tutelato anche a norma della direttiva 2013/40/UE[303].

Lo studio del regolamento (UE) 2019/881 ha evidenziato come l'ENISA, abbandonato ormai il ruolo di mero gregario - che la connotava in forza del regolamento istitutivo (CE) 460/2004 - oggi cooperi a livello paritario con gli Stati membri e stabilisca sinergie con le Istituzioni, gli Organi e le Autorità di vigilanza dell'Unione, che si occupano della tutela della vita privata e della protezione dei dati personali, al fine di contrastare i *cybercrimes*. La cooperazione avviene scambiando conoscenze e *best practises*, fornendo consulenze e orientamenti agli Stati per l'esecuzione di compiti specifici e contribuendo alla formazione di una *cultura cibernetica* a favore degli utenti[304].

L'esame del *Cybersecurity Act*, inoltre, ha evidenziato come l'Unione europea riconosca, a tutti gli effetti, il ruolo essenziale rivestito nella società odierna dalle reti, dai sistemi informativi e dai servizi di comunicazione elettronica, che sono veri e propri pilastri della crescita economica. Le tecnologie cibernetiche dell'informazione e della comunicazione sono ormai indefettibile presupposto rispetto allo svolgimento delle attività quotidiane nel contesto dei cosiddetti *settori essenziali dello Stato* (i quali partecipano della sua Personalità), quali la sanità, l'energia, la finanza, i trasporti, la politica[305].

---

[303] Sul rapporto sussistente fra cyberterrorismo e «sistema di informazione» si veda S. C. MCQUADE, *Encyclopedia of Cybercrimes,* op. cit., p. 55, in cui si legge che: «The goal of so called cyberterrorism is to attack information systems to instill fear on those who have the capability to make political changes deemed necessary by the attackers».

[304] La cooperazione operativa fra l'ENISA e gli Stati si svolge (art. 7, par. 4 del regolamento 2019/881) attraverso: a) consigli su come migliorare le loro capacità di prevenzione e rilevazione degli incidenti e di risposta agli stessi; b) l'assistenza, su richiesta di uno o più Stati membri, nella valutazione di incidenti aventi un impatto rilevante o sostanziale, tramite la messa a disposizione di competenze e l'agevolazione della gestione tecnica di tali incidenti; c) l'analisi delle vulnerabilità e degli incidenti sulla base delle informazioni pubblicamente disponibili o delle informazioni fornite volontariamente dagli Stati membri a tale scopo; d) il sostegno in relazione a indagini tecniche *ex post* sugli incidenti aventi un impatto rilevante o sostanziale ai sensi della direttiva (UE) 2016/1148.

[305] Considerando n. 1 del regolamento (UE) 2019/881.

Tuttavia, sebbene il legislatore europeo preveda l'inesorabile aumento delle tecnologie cibernetiche nei settori predetti, attualmente tale sviluppo non pare essere controbilanciato da un adeguato livello di *cybersicurezza* nei diversi ordinamenti nazionali[306]. Questi devono dunque prendere consapevolezza di tale deficienza ed adeguarsi, quanto prima, agli *standards* europei. È intuibile, del resto, come l'incremento della digitalizzazione e della connettività comporti maggiori rischi e, quindi, una maggiore vulnerabilità rispetto alle minacce informatiche, specie quelle provenienti da associazioni con finalità di terrorismo, le quali si avvalgono del *cyberspace* per porre in essere condotte che, per la loro *natura* o *contesto*, possono arrecare grave danno ad un Paese, allo scopo precipuo di distruggerne le strutture fondamentali (art. 1 della decisione-quadro 2002/475/GAI)[307].

La lettura del *Cybersecurity Act* attraverso la lente della *Strategia antiterrorismo europea* elaborata nel 2005[308] conferma che la *cybersecurity* non

---

[306] Sul punto si veda L. EDWARDS, B. SCHAFER, E. HARBINJA, *Future law. Emerging technology, regulation and ethics*, op. cit., p. 70, in cui gli autori prospettano uno scenario in cui gli uomini vivranno in ambienti domestici cibernetici: «home hubs with digital facial expressions that prompt guilt or contentment by smiling or scowling at you; conversational agents that hang on to your every world and unanswerable query; intelligent fridges that monitor your food consumption habits to suggest *sui generis* recipes that help avoid more food waste (perhaps by mixing together that pot of leftover fizzy hummus and curdled milk); smart lighting that can create the perfect *hygge* mood or Monday night mosh pit (depending on how your day went); and smart security systems that let you in, just because 'your face fits', despite forgetting your RFID entry fob». Tuttavia gli autori sono certi che l'attuale legislazione degli ordinamenti nazionali degli Stati europei non sia pronta per disciplinare un simile scenario, onde ritengono che «regulators and lawyers also need to exercise their imaginations to create strategies that move beyond the headline», al fine di garantire un'efficace *cybersecurity*.

[307] Considerando n. 3 del regolamento del *Cybersecurity Act*.

[308] La *Strategia* elenca le priorità fondamentali della prevenzione del terrorismo, anche cibernetico, tra le quali spiccano: affrontare l'incitamento alla violenza ed il reclutamento segnatamente negli ambienti che più possono favorirli come, ad esempio, le prigioni ei luoghi di culto o di formazione religiosa, segnatamente adottando una normativa che definisca reati tali comportamenti; sviluppare un dialogo interculturale che coinvolga anche Stati terzi rispetto all'Unione europea; proseguire la ricerca, mettere in comune le analisi e le esperienze per approfondire la comprensione delle questioni ed elaborare risposte. Per un'elencazione completa delle priorità fondamentali da perseguire attraverso la prevenzione si veda *The European Union Counter - Terrorism Strategy*, op. cit., p. 9 (punto 13), in cui oltre a quelle già menzionate, si fa altresì riferimento a: sviluppare approcci comuni nell'individuare e affrontare comportamenti

costituisce più soltanto un fatto dai profili squisitamente tecnici, risultando invece «una questione in cui il comportamento umano è (n.d.r. almeno) di pari importanza» rispetto a detti profili[309]. Nella summenzionata *Strategia* viene dunque proposta una forma di prevenzione che può dirsi *sociale* (c.d. *social crime prevention*) - già nota agli ordinamenti di *common law* – con la quale il legislatore europeo si prefigge di impedire la radicalizzazione (oggi prevalentemente *online*), l'accoglimento del messaggio propagandato e, più in generale, l'affiliazione a gruppi terroristici con un intervento "a monte", neutralizzando cioè i fattori genetici di tipo socioculturale del terrorismo[310].

Tale ambizioso obiettivo può essere efficacemente perseguito attraverso l'impiego di misure che, pur dovendo intervenire necessariamente prima del delitto – per scongiurarne la commissione – devono essere dotate di una forza e di una pervasività proporzionata al disvalore del terrorismo cibernetico.

Trattasi delle *misure di prevenzione*, alle quali tradizionalmente l'ordinamento italiano riconosce natura sostanzialmente penale ma formalmente amministrativa. Detti strumenti, pur possedendo una forza equivalente a quella della pena (potendo limitare anche significativamente la libertà personale del destinatario), intervengono in fase predelittuale e, quindi, pre-processuale. Il presupposto applicativo delle misure in parola non è dunque l'accertamento della responsabilità per la commissione di un reato, sulla base delle prove formate in dibattimento nel contraddittorio delle parti davanti ad un giudice.

---

problematici, in particolare l'uso di Internet a fini illegali; sviluppare una strategia riguardo ai media e la comunicazione per illustrare meglio le politiche dell'UE; sviluppare un linguaggio non emotivo per discutere questi temi.

[309] Considerando n. 8 del regolamento: «La cybersicurezza non costituisce soltanto una questione relativa alla tecnologia, ma anche una in cui il comportamento umano è di pari importanza. Di conseguenza, è opportuno promuovere energicamente l'*igiene informatica*, vale a dire semplici misure di *routine* che, se attuate e svolte regolarmente da cittadini, organizzazioni e imprese, riducono al minimo la loro esposizione a rischi derivanti da minacce informatiche».

[310] Il riferimento è ai tre fattori previsti in *The European Union Counter - Terrorism Strategy*, op. cit., p. 9 (punto 11) e precisamente: a) uno Stato dotato di una Personalità debole o, all'estremo opposto, autocratica; b) una modernizzazione rapida ma giuridicamente incontrollata; c) l'assenza di prospettive politiche ed economiche, nonché di opportunità di istruzione.

Al contrario rilevano presupposti applicativi diversi (non aventi valore di prova *strictu sensu*), fra tutti la *pericolosità sociale* del soggetto proposto, da valutare in concreto. In particolare è necessario indagare il significato che la *pericolosità* assume in ambito cibernetico, nonché i rapporti che la legano, ad esempio, ai fattori sintomatici del contesto di radicalizzazione che deve connotare le condotte terroristiche. Infatti le misure di prevenzione, a cui fa riferimento la *Strategia antiterrorismo europea*, sono volte ad incidere sugli elementi della «natura» e del «contesto», i quali - secondo la definizione di cui all'art. 1 della decisione-quadro 2002/475/GAI (e, quindi, dell'art. 270-*sexies* c.p.) - rappresentano l'essenza dei reati terroristici sotto il profilo oggettivo, atteso che la capacità delle condotte terroristiche di arrecare grave danno ad un Paese o ad un'organizzazione internazionale dipende proprio da tali due elementi.

Infine, il regolamento (UE) 2021/784 prevede l'introduzione dei cosiddetti «*ordini di rimozione*», ovverosia misure che consentono alle Autorità competenti di ordinare ai prestatori di servizi di *hosting* di rimuovere i contenuti pubblicati *online* - ed in particolare sulle piattaforme di loro competenza – che risultano essere terroristici, ai sensi dell'art. 2, n. 7 del regolamento. Tale natura dei contenuti deve essere accertata sulla base di una *valutazione in concreto*, che tenga conto dei parametri previsti dal Considerando n. 11 del regolamento, al fine di evitare che la scelta dei contenuti da rimuovere venga delegata ad automatismi basati su algoritmi, che comporterebbero una palese violazione del principio di offensività.

L'esame delle principali fonti europee in materia di *cybercrimes* e di terrorismo ha permesso di osservare che la *strategia europea multilivello* per il contrasto preventivo del terrorismo cibernetico presupponga che le infrastrutture critiche cibernetiche dello Stato siano connotate dalla *cyberresilienza*. Questa - lungi dal consistere nella mera resistenza - racchiude in sé le capacità di prevenire i reati di terrorismo cibernetico, di prepararsi alla loro commissione e di assorbire gli eventuali effetti dannosi degli stessi, adattandosi senza interrompere i servizi

erogati (pena arrecare grave danno al Paese)[311]. Ad ogni buon conto è doveroso segnalare che, finora, l'importanza assunta in ambito penale dalla cyberresilienza non è stata debitamente approfondita dalla dottrina che si dedica allo studio dei *cybercrimes*. Diversamente il legislatore europeo ha dimostrato particolare attenzione per il tema, tanto da adottare le proposte di una *direttiva sulla resilienza delle entità critiche* e di una direttiva *NIS 2* per aggiornare la precedente direttiva 2016/1148[312].

[311] D. STASIO, *La lotta multilivello al terrorismo internazionale*, Giuffrè, pp. 242 e ss., in cui l'autore descrive la strategia multilivello contro il terrorismo approntata dal legislatore europeo, soffermandosi peculiarmente sulla prevenzione.

[312] Le Istituzioni europee si sono dimostrate consapevoli della gravità dell'attuale lacuna in materia di cyberresilienza e pertanto, in data 16.12.2020, la Commissione ha presentato la *Proposta di direttiva sulla resilienza dei soggetti critici* (COM(2020) 829 final.), disponibile al seguente *link*: *https : / / eur – lex . europa . eu /legal – content / IT / TXT / PDF / ?uri = CELEX : 52020PC0829&from = IT*. In particolare, da quanto si legge nella relazione che accompagna la proposta, questa «rispecchia gli approcci nazionali in un numero crescente di Stati membri, che tendono a porre l'accento sulle interdipendenze intersettoriali e transfrontaliere e che sono sempre più improntati al concetto di resilienza, in cui la protezione è solo uno degli elementi accanto alla prevenzione e all'attenuazione dei rischi, alla continuità operativa e alla ripresa. Dato che le infrastrutture critiche corrono anche il rischio di essere potenziali bersagli terroristici, le misure volte a garantire la resilienza dei soggetti critici contenute nella presente proposta contribuiscono alla realizzazione degli obiettivi della recentemente adottata agenda dell'UE per la lotta al terrorismo».

CAPITOLO III

Profili critici della disciplina italiana delle misure di prevenzione: adeguamenti, de iure condendo, per il contrasto del cyberterrorismo

SOMMARIO: 1. Gli strumenti special-preventivi alternativi alla pena: le misure di prevenzione. – 1.1. Le misure di prevenzione personali. – 1.2. Le misure di prevenzione patrimoniali, in particolare l'*asset freezing* contro il terrorismo. – 2. Il sistema delle fonti delle misure di prevenzione nell'ordinamento italiano. – 3. I presupposti soggettivi per l'applicazione delle misure di prevenzione: l'appartenenza del soggetto alle categorie "terroristiche" (art. 4 del d.lgs. 159 del 2011). – 3.1. La pericolosità sociale del prevenuto. – 3.2. Il giudizio di pericolosità. – 4. Le misure di prevenzione al vaglio della giurisprudenza europea e domestica. – 4.1. La sentenza della Corte europea dei diritti dell'uomo del 23 febbraio 2017, De Tommaso c. Italia (ricorso n. 43395/09). – 4.2. Osservazioni critiche sulla sentenza De Tommaso. – 4.3. La sentenza 24 gennaio 2019, n. 24 della Corte Costituzionale: il dialogo "*mediato*" tra la Corte europea e quella nazionale. – 5. Le misure di prevenzione contro le condotte con finalità cyberterroristiche. – 5.1. I presupposti soggettivi delle misure di prevenzione per il contrasto del cyberterrorismo. - 5.1.1. La categoria dei destinatari delle misure di prevenzione contro il cyberterrorismo. – 5.1.2. La "pericolosità sociale cibernetica" ed i criteri per il suo accertamento nell'apposito giudizio. – 5.2. Le singole misure di prevenzione contro il cyberterrorismo: spunti dal diritto sovranazionale e nazionale. – 5.2.1. Le misure di prevenzione di matrice eurounitaria contro il cyberterrorismo. – 5.2.2. Spunti di riflessione per le misure di prevenzione contro il cyberterrorismo dal settore militare e dell'*Intelligence*. – 5.2.3. Le misure di prevenzione dei reati cibernetici nella legislazione speciale: il modello di organizzazione, gestione e controllo previsto dal d.lgs. 231/2001 sulla responsabilità da reato delle persone giuridiche. – 5.2.4. Le misure di prevenzione dei reati cibernetici nella legislazione speciale: la legge 71/2017 sulla prevenzione ed il contrasto del fenomeno del cyberbullismo. – 5.3. Le misure di prevenzione

positiva. In particolare il modello di prevenzione positiva sociale e situazionale. – 6. Le misure di prevenzione positiva contro il cyberterrorismo. Osservazioni conclusive.

1. Gli strumenti special-preventivi alternativi alla pena: le misure di prevenzione.

L'ordinamento italiano prevede specifici *strumenti alternativi alla pena* per il perseguimento della *funzione special-preventiva* che operano *ante delictum*: le *misure di prevenzione*[313].

Esse possono essere negative o positive.

Le prime, maggiormente diffuse nell'ordinamento italiano, comportano restrizioni, più o meno dirette, della libertà personale o, più in generale, privazioni di diritti individuali[314]. Le seconde, invece (largamente diffuse nei Paesi di *common law*), consistono in interventi che perseguono il fine preventivo attraverso la promozione dei diritti fondamentali dei consociati e, quindi, nella creazione di migliori condizioni di vita e maggior benessere sociale[315].

Secondo autorevole dottrina, l'impiego delle misure di prevenzione dovrebbe preferirsi alla pena, dal momento che la dilatazione a fini prevenzionistici della stessa comporta una caduta di livello della serietà e dell'efficacia del sistema penale nel suo insieme, perché strumentalizza ingiustamente e banalizza al contempo il rimprovero che è intrinsecamente inerente alla pena[316].

---

[313] L. PASCULLI, *Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali*, Padova University Press, 2012, pp. 99 e ss.; F. MENDITTO, *Misure di prevenzione personali e patrimoniali,* Giuffrè, 2019, pp. 1 e ss.

[314] F. BRIZZI, P. PALAZZO, A. PERDUCA, *Le nuove misure di prevenzione personali e patrimoniali. Dopo il Codice antimafia (D.lgs. 159/2011)*, Maggioli, 2012, pp. 7 e ss.

[315] L. PASCULLI, *Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali*, op. cit., pp. 109 e ss.

[316] M. RONCO, *Appunti di diritto penale,* Libreria Progetto Padova, 2014, p. 248. Per un esame critico della funzione special-preventiva della pena, invece, M. PAVARINI, *La pena*

Le misure di prevenzione dovrebbero preferirsi alla pena anche perché il suo impiego in funzione precipuamente special-preventiva ha comportato, specie in materia di legislazione antiterrorismo (come evidenziato nel Capitolo I del presente lavoro), l'iperproduzione di fattispecie di reato costruite con l'impiego di tecniche incriminatrici che prevedono la combinazione degli istituti del *pericolo presunto* e del *dolo specifico*, al fine di dilatare in senso anticipatorio la rilevanza penale - con l'incriminazione di atti anteriori sinanco alla soglia del tentativo punibile *ex* art. 56 c.p. - le quali si pongono in contrasto con i principi di *materialità*, *offensività* e *colpevolezza*.

Il tratto distintivo delle misure in parola è rappresentato dai presupposti necessari per la loro applicazione e, in particolare, dalla *pericolosità sociale* del loro destinatario, che non presuppone la previa commissione di un reato[317].

La sussistenza della pericolosità sociale in capo al destinatario della misura deve essere valutata dall'Autorità Giudiziaria o Amministrativa attraverso un apposito giudizio. Tuttavia questo, a differenza del processo penale, non si fonda su elementi probatori in senso stretto, dal momento che non è volto ad accertare la responsabilità per un fatto di reato, riguardando atti anteriori alla sua commissione ed essendo finalizzato ad irrogare misure atte a prevenirla[318].

«utile», la sua crisi e il disincanto: verso una pena senza scopo, in *Rassegna Penitenziaria e criminologica*, 1/1983, pp. 16-23.

[317] L. PASCULLI, *Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali*, op. cit., pp. 15-16. L'autore precisa che l'assenza della previa commissione di un fatto di reato, come presupposto per l'applicazione delle misure di prevenzione, comporta che le stesse vengano anche definite misure *praeter*, *extra*, *sine* o *ante delictum*. Il criterio cronologico, relativo all'intervento predelittuale delle misure di prevenzione, rappresenta il principale elemento differenziatore fra queste e le misure di sicurezza. Le seconde, infatti, sono rivolte a favorire il reinserimento e la rieducazione delle persone socialmente pericolose, le quali abbiano già commesso un reato. Nello stesso senso T. PADOVANI, *La pericolosità sociale sotto il profilo giuridico*, in *Trattato di criminologia, medicina criminologica e psichiatria forense*, a cura di F. FERRACUTI, vol. XIII, Giuffrè, 1990, pp. 313 e ss.

[318] Per un esame del giudizio di pericolosità si rinvia a A. MARTINI, *Essere pericolosi. Giudizi soggettivi e misure personali*, Giappichelli, 2017, pp. 149 e ss., L. DELLA RAGIONE, *Le misure di prevenzione nello specchio del volto costituzionale del sistema penale*, in *Discrimen*, 20.4.2020, p. 9.

Rileva osservare che in molti ordinamenti stranieri, specie quelli di *common law*, trovano larga applicazione le misure di *prevenzione positiva*, le quali, intervenendo *ante delictum*, mirano a ridurre le occasioni di delinquenza precipuamente attraverso la promozione dell'integrazione sociale del destinatario[319]. La *positive prevention* può attuarsi, ad esempio, mediante *programmi di assistenza sociale*, *programmi formativi*, *premi* e *incentivi* mirati alla promozione del rispetto della legalità o attraverso mezzi di difesa e di controllo generici[320].

Come emerso dall'esame degli atti di diritto derivato condotto nel precedente capitolo di questo lavoro, il legislatore europeo spinge, con sempre maggiore insistenza, verso l'adozione di misure di *prevenzione positiva*, che consentano di intervenire a monte e, precisamente, sulle *cause di tipo sociale*, *politico e culturale* di un determinato fenomeno criminoso, azzerandone ogni idoneità criminogena[321].

Ad oggi l'ordinamento italiano continua a prediligere le misure negative, le quali, secondo la tradizionale *summa divisio*, si diversificano in *personali* e *patrimoniali*, in base agli interessi sui quali incidono.

---

[319] L. PASCULLI, *Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali*, op. cit., p. 104, in particolare nota 22, in cui l'autore evidenzia che, mentre in certi Paesi «*crime prevention* è sinonimo di prevenzione positiva, in altri lo strumento prevalente di prevenzione sono misure negative». Tra questi ultima figura l'Italia.

[320] Sul punto M. PELISSERO, *Diritto penale - Appunti di parte generale*, Giappichelli, 2021, pp. 10 e 11.

[321] Per un esame approfondito delle misure di prevenzione positiva si rinvia a L. PASCULLI, *Le misure di prevenzione del terrorismo*, op. cit., p. 109 e ss. L'autore spiega che, attualmente, le *misure di prevenzione positiva* sono oggetto, da parte della dottrina italiana, di studi per lo più di tipo criminologico e sociologico. Infatti la scienza penale continua ad interessarsi, in via principale, delle *misure di prevenzione negativa*, in virtù dei loro contenuti, prossimi - se non coincidenti - con quelli della pena. L'interesse del penalista rispetto a queste misure, per altro, è sollecitato dal progressivo sviluppo di articolati sistemi di prevenzione negativa, che molti Paesi stranieri hanno recentemente impiegato per il contrasto del terrorismo internazionale (ivi, p. 17).

1.1. Le misure di prevenzione personali

Le misure di prevenzione personali incidono direttamente sulla libertà della persona e si distinguono in *privative* e *restrittive* della libertà personale.

Le prime comprendono tutti i provvedimenti amministrativi, giudiziari, emergenziali od ordinari - terapeutici o meramente custodiali - che, in modo sostanzialmente analogo alla pena della reclusione, deprivano il soggetto, ritenuto pericoloso, della sua libertà materiale[322].

Tali strumenti sono stati ampiamente utilizzi nei sistemi emergenziali antiterrorismo dei Paesi di *common law* (Stati Uniti d'America e Regno Unito in testa)[323], legittimando la detenzione dei soggetti - soltanto sospettati di essere terroristi - sulla base di provvedimenti dell'Autorità amministrativa, per fini esclusivamente investigativi e comunque «*without charge*»[324].

---

[322] Le misure di prevenzione personali privative della libertà sono comunemente definite *detenzione o carcerazione preventiva.* Ad ogni modo, giova osservare che il termine viene utilizzato, in generale, per riferirsi a tutte le forme di detenzione che intervengono prima di una condanna che accerti la penale responsabilità del detenuto, ricomprendendovi, quindi, anche la misura della custodia cautelare in carcere. Tuttavia questa, come noto, risponde ad una *ratio* diversa da quella delle misure di prevenzione, postulando, da un lato, i presupposti previsti dagli artt. 273 e 280 c.p.p. e, dall'altro lato, le esigenze cautelari *ex* art. 274 c.p.p.

[323] L. PASCULLI, *Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali*, op. cit., pp. 138 e ss.

[324] Con le espressioni «*imprisonment without charge*» o «*indefinite detention*» viene comunemente fatto riferimento a forme di carcerazione che non postulano la previa condanna da parte dell'Autorità giudiziaria, all'esito di un processo che accerti la penale responsabilità del detenuto. Per un esame della «*indefinite detention*» si consiglia la lettura di A. DE ZAYAS*, Human rights and indefinite detention*, in *International review of the red cross*, vol. 87, 2005, pp. 6 e ss., in cui l'autore precisa che tale forma di carcerazione è stata impiegata dal Regno Unito e dagli Stati Uniti d'America precipuamente per contrastare il terrorismo nel contesto della cosiddetta «*war of terror*» e per questo è stata riservata a particolari categorie di soggetti, tra i quali figurano proprio i terroristi. Ad ogni buon conto l'autore aggiunge che non vi è dubbio che la «*indefinite detention*» costituisca un trattamento inumano, il quale, al ricorrere di determinate circostanze, può configurare anche una forma di tortura. Con particolare riferimento alla carcerazione come misura di prevenzione impiegata negli ordinamenti stranieri si veda S. FRANKOWSKI, D, SHELTON, *Preventive Detention. A Comparative and International perspective*, Martinus Nijhoff, 2022, pp. 1-53 e peculiarmente in quello statunitense *Ibidem*, pp. 53-113.

Per quanto attiene al diritto eurounitario, la Corte europea dei diritti dell'uomo ha riconosciuto la compatibilità delle misure in parola rispetto alla Convenzione europea dei diritti dell'uomo, purché la loro applicazione avvenga nel rispetto delle rigorose condizioni dettate dall'art. 5, par. 1, CEDU[325].

La disposizione, dopo aver sancito il diritto alla *libertà* (enunciandone l'intangibilità) e quello alla *sicurezza*, indica i casi in cui è possibile privare la persona del primo (lettere da a ad f). Orbene, fatta eccezione per le previsioni contenute nella seconda parte dell'art. 5, par. 1 - attinenti a casi particolari (lettere d, e, f)[326] - le lettere a, b e c della disposizione consentono di privare un soggetto della libertà soltanto *post delictum* e, più precisamente, sul presupposto della condanna di un Tribunale per la commissione di un illecito penale (art. 5, par. 1, lett. a e b) o, quantomeno, di motivi plausibili e fondati che consentano di sospettare che egli abbia commesso un reato o di ritenere che sia necessario impedirgli di commetterlo o, ancora, che possa darsi alla fuga dopo averlo commesso (art. 5, par. 1, lett. c).

Ad ogni buon conto, nell'attuale panorama italiano, non sono rintracciabili strumenti di prevenzione tanto afflittivi, i quali trovavano un corrispondente nel

---

[325] Corte EDU, sent. 6.11.1980, Guzzardi c. Italia, in cui i giudici hanno accertato la violazione dell'art. 5, par. 1, CEDU, nel caso di una persona sottoposta all'obbligo di soggiorno nell'isola dell'Asinara, trattandosi «di assegnazione di una persona ritenuta socialmente pericolosa al soggiorno obbligato in un'isola, ove possa muoversi soltanto in una zona estremamente esigua, sotto permanente sorveglianza e nella quasi completa impossibilità di stabilire contatti sociali». In particolare, i giudici non hanno ravvisato nessuna delle cause legittimanti la privazione della libertà a norma dell'art. 5, par. 1, CEDU. Inoltre sulle condizioni che rendono compatibili le misure di prevenzione personali privative della libertà con i principi del diritto dell'Unione europea ed in particola della Convenzione europea dei diritti dell'uomo si veda A. BALSAMO, *Diritto dell'UE e della CEDU e confisca di prevenzione*, in *Il Libro dell'anno del diritto*, Istituto della Enciclopedia Italiana, 2014, pp. 675 e ss.; F. MENDITTO, *Misure di prevenzione patrimoniali e Cedu*, in *Quest. Giust*., 2014, p. 41 ss.

[326] La lettera d) dell'art. 5, par. 1, CEDU ammette che si possa limitare la libertà di un minore al fine di sorvegliare la sua educazione oppure di tradurlo dinanzi all'autorità competente; la successiva lettera e), invece, ammette la detenzione regolare di una persona che sia suscettibile di propagare una malattia contagiosa, di un alienato, di un alcolizzato, di un tossicomane o di un vagabondo; infine la lettera f) della stessa disposizione consente di arrestare o detenere una persona al fine di impedirle di entrare illegalmente nel territorio dello Stato.

ricovero negli ospedali psichiatrici giudiziari, definitivamente chiusi a far data dal 31 marzo 2015[327].

Le *misure di prevenzione personali restrittive*, invece, non privano totalmente il soggetto della sua libertà, ma la limitano solamente e si distinguono in *interdittive*, il cui contenuto consiste nella previsione di specifici divieti o nella sorveglianza nei confronti del destinatario, e *prescrittive*, le quali prevedono obblighi di *facere*, stabilendo l'osservanza di un ben preciso comportamento[328].

Parimenti alle misure di prevenzione personali privative della libertà, anche quelle limitative hanno avuto ampia diffusione nei sistemi emergenziali per il contrasto del terrorismo dei *Paesi di common law*.

In proposito si pensi ai *control orders,* adottati dal Regno Unito con il *Prevention of Terrorism Act* del 2005 e sostituiti dalle cosiddette *monitoring measures*, previste dal *Terrorism Prevention and Investigation Measures Act* del 2011. In particolare i *Control orders* consistevano in provvedimenti dell'Autorità amministrativa, che potevano avere i contenuti più vari, quali, solo a titolo esemplificativo, la limitazione della libertà di associazione e di movimento oppure la restrizione nell'utilizzo di apparecchi telefonici e di piattaforme *online*[329]. Le *monitoring measures*, invece, si distinguevano dalle prime per la necessità della previa autorizzazione dell'Autorità giudiziaria, salvo nei casi di particolare urgenza - in cui potesse ragionevolmente ritenersi che un soggetto fosse stato

---

[327] La chiusura degli ospedali psichiatrici giudiziari è stata disposta con il d.l. 22.12.2011, n. 211, recante "*Interventi urgenti per il contrasto della tensione detentiva determinata dal sovraffollamento delle carceri*", che l'aveva fissata entro il 31.3.2013. Successivamente il d.l. 25.3.2013, n. 24 aveva prorogato la chiusura al 1.4.2014 e, infine, il d.l. 31.3.2014, n. 52 aveva previsto un'ulteriore proroga annuale al 31.3.2015, data di chiusura definitiva degli ospedali psichiatrici giudiziari.

[328] P. PITTARO, *Misure di prevenzione personali e sistema penale*, in AA.VV., F. FIORENTIN (a cura di), *Le misure di prevenzione personali e patrimoniali*, op. cit., pp. 207 e ss., in cui l'autore evidenzia le differenze intercorrenti fra misure di prevenzione *detentive* e misure di prevenzione *non detentive*. Giova in ogni caso evidenziare che le misure restrittive della libertà personale sono spesso accompagnate da prescrizioni volte a consentire un penetrante controllo della polizia, talvolta anche attraverso strumenti elettronici, per monitorare i movimenti del prevenuto.

[329] L. PASCULLI, *Le misure di prevenzione del terrorismo e dei traffici criminosi internazionale*, op. cit., pp. 147-149.

coinvolto in attività terroristiche – in relazione ai quali la misura poteva essere disposta direttamente dall'Autorità amministrativa, in particolare dal *Secretary of State*[330].

Le *misure di prevenzione personali restr*ittive della libertà sono disciplinate dall'art. 2, del protocollo addizionale n. 4 alla Convenzione europea dei diritti dell'uomo, che, nel sancire il diritto alla libertà di circolazione e quello alla fissazione della residenza sul territorio nazionale, indica i casi in cui tali diritti possano subire limitazioni. In particolare, il par. 3 del summenzionato articolo prevede che le misure restrittive devono: a) essere oggetto di un'espressa previsione legislativa; b) essere funzionali alla tutela di interessi giuridici particolarmente rilevanti[331]; c) rispettare la proporzionalità fra il diritto limitato e le esigenze della collettività che ne rendono necessaria la limitazione[332].

L'ordinamento italiano, attualmente, prevede esclusivamente *misure di prevenzione personali limitative della libertà*, disciplinate dal d.lgs. 6.9.2011, n. 159 (c.d. *Codice Antimafia*), ovverosia il *rimpatrio con foglio di via obbligatorio* (art. 2), l'*avviso orale* (art. 3) e la *sorveglianza speciale di pubblica sicurezza* (art. 6, co. 1), alla quale possono essere affiancati il *divieto* (art. 6, co. 2) o *l'obbligo* (art. 6, co. 3) *di soggiorno*[333].

---

[330] L. PASCULLI, *ibidem*, in cui l'autore enuclea dettagliatamente le diverse tipologie di *monitoring meausres*: a) obblighi di soggiorno nella località di residenza o in altra ritenuta appropriata dall'autorità; b) obbligo di non lasciare il Regno Unito; c) divieti e limitazioni di accesso a determinati luoghi; d) obblighi di seguire le indicazioni impartite dai *constables* circa la propria libertà di movimento; e) restrizioni circa il possesso e l'utilizzo di strumenti di comunicazione elettronica (computer, telefoni, ecc.); f) divieti e limitazioni di associazione e comunicazione con determinate persone; g) divieti e limitazioni alle attività lavorative e di studio; h) obbligo di presentarsi presso un posto di polizia in tempi e luoghi determinati.

[331] L'art. 2, par. 3 del protocollo addizionale n. 4, CEDU individua gli interessi che possono legittimare la restrizione della libertà personale: a) sicurezza nazionale; b) pubblica sicurezza; c) ordine pubblico; d) prevenzione dalle infrazioni penali; e) salute, morale o libertà altrui.

[332] Per un'applicazione del principio di proporzionalità in riferimento al trattamento dei dati personali in funzione di prevenzione del terrorismo si veda B. PIATTOLI, *Principio di proporzionalità UE e trattamento dei dati personali nella lotta al terrorismo*, in *Dir. Pen. e Proc*., 7/2015, pp. 885-894.

[333] Ulteriori misure che possono essere irrogate unitamente alla sorveglianza speciale di pubblica sicurezza sono il *divieto di ingresso nel territorio nazionale* e l'*espulsione degli stranieri*.

1.2. Le misure di prevenzione patrimoniali, in particolare l'asset freezing contro il terrorismo

Le misure di prevenzione patrimoniali (dette anche reali) incidono sul patrimonio del destinatario e, quindi, solo indirettamente sulla sua libertà personale.

Esse vengono tradizionalmente suddivise in *specifiche* e *generiche*.

Le prime, che possono essere temporanee o definitive, incidono sulla proprietà o sulla disponibilità di beni materiali o di somme di denaro.

Le seconde, invece, limitano le attività del destinatario che attengono alla conservazione ed all'accrescimento del patrimonio[334].

L'interesse per le misure di prevenzione patrimoniali ha recentemente ricevuto nuovo impulso nel diritto europeo, che, nel recepire le risoluzioni del Consiglio di sicurezza delle Nazioni Unite in materia di contrasto del terrorismo[335], ha previsto l'introduzione di nuove *smart sanctions*, operanti *ante delictum*, da irrogare a soggetti ricompresi in apposite *black lists*, le quali devono essere aggiornate dal Consiglio dell'Unione europea almeno una volta per

---

Sul punto M. PELISSERO, *Il vagabondo oltre confine. Lo statuto penale dell'immigrato nello Stato di prevenzione*, in *Politica del diritto*, Vol. II, 2011, pp. 239 e ss., in cui l'autore evidenzia che tali misure - trovando applicazione soprattutto nel diritto dell'immigrazione - rischiano di riproporre le logiche esclusive che, un tempo, riguardavano gli oziosi e soprattutto i vagabondi oltre confine (ricorrenti nella versione originaria della l. 27.12.1956, n. 1423), che la Consulta ha dichiarato costituzionalmente illegittime.

[334] Per un esame delle misure di prevenzione patrimoniali in generale, F. MENDITTO, *Le misure di prevenzione personali e patrimoniali*, op. cit., pp. 279 e ss.; A. BALSAMO, V. D'AGOSTINO, *Inquadramento sistematico ed evoluzione storica delle misure di prevenzione patrimoniali*, in AA.VV., F. FIORENTIN (a cura di), *Le misure di prevenzione personali e patrimoniali*, op. cit., pp. 501 e ss.

[335] Trattasi delle risoluzioni n. 1267/1999 e n. 1373/2001, entrambe dedicate alle misure patrimoniali per il contrasto del terrorismo. In particolare, la prima risoluzione ha introdotto il *Comitato per le sanzioni contro Al-Qaeda ed i Talebani*, mentre la seconda ha previsto un *Comitato per le sanzioni contro il terrorismo* in generale. Entrambi i Comitati, sulla base di informazioni che raccolgono presso gli Stati membri attraverso le Autorità competenti, redigono e gestiscono apposite liste contenenti i nominativi di persone, entità e gruppi sospettati di essere coinvolti in atti terroristici. Dall'inserimento del nominativo nella lista consegue l'applicazione di una serie di misure restrittive, tra le quali il *congelamento di capitali*, il *travel ban* e l'*embargo*.

semestre, al fine di accertare che la permanenza dei soggetti nelle stesse sia giustificata[336].

Il fondamento normativo delle *smart sanctions* risiede nell'art. 75 TFUE, il quale dispone che, per la prevenzione e la lotta contro il terrorismo e le attività connesse, il Parlamento europeo e il Consiglio, mediante regolamenti deliberati secondo la procedura legislativa ordinaria, definiscono un insieme di misure amministrative concernenti i movimenti di capitali ed i pagamenti.

Esempio emblematico di *smart sanction* per il contrasto dei reati con finalità di terrorismo, adottata a livello europeo, è il cosiddetto *asset freezing*. Questo consiste in un *congelamento* dei beni del destinatario, con un contenuto sostanzialmente analogo a quello dell'istituto del *sequestro* noto all'ordinamento italiano. Tuttavia, diversamente da questo, l'*asset freezing* può protrarsi anche per lassi temporali ultradecennali, realizzando, di fatto, una vera e propria espropriazione di capitali[337].

L'art. l, par. 2 del regolamento n. 2580 del 27.12.2001 (relativo a misure restrittive specifiche, contro determinate persone ed entità, destinate a combattere

---

[336] Sul punto si veda CGUE, Grande Sezione, sent. 23.11.2021, C-833/19 P, in cui i giudici hanno esaminato le condizioni per la permanenza di un'organizzazione (nel caso di specie *Hamas*) nell'elenco delle persone, dei gruppi e delle entità coinvolti in atti terroristici (c.d. *black list*).

[337] Per un esame della misura dell'*asset freezing* si rinvia a C. BATTAGLINI, *Le misure patrimoniali antiterrorismo alla prova dei principi dello stato di diritto*, in *Dir. Pen. Cont.*, 1/2017, p. 59; L. G. BRUNO, *Misure di prevenzione patrimoniali e congelamento dei beni per reati di terrorismo: problemi sostanziali e processuali*, in *Dir. Pen. Proc.*, 2007, pp. 99 e ss.; A. MANGIARACINA, *Il "congelamento dei beni" e la confisca come misure di contrasto alla criminalità organizzata transnazionale e al terrorismo*, in AA.VV., *La Giustizia patrimoniale penale*, UTET, 2011, pp. 990 e ss. La risoluzione n. 1267/1999 del Consiglio di Sicurezza delle Nazioni Unite, che ha introdotto la misura dell'*asset freezing* senza definirla, prevedeva che essa dovesse applicarsi solamente nei confronti dei talebani e delle persone ritenute collegate alla rete terroristica di Al-Qaeda. La successiva risoluzione n. 1373/2001, che estende la misura del congelamento, in via generale, a tutti i soggetti sospettati di appartenere o di sostenere organizzazioni terroristiche, prevede che gli Stati debbano impegnarsi a prevenire e reprimere il finanziamento degli atti di terrorismo e a congelare, senza indugio, fondi, beni finanziari e risorse economiche di persone che commettono - o tentano di commettere - atti terroristici oppure che partecipino alla loro realizzazione; di entità di proprietà di o controllate direttamente o indirettamente da tali persone; di persone ed entità che agiscono a nome di (o agli ordini di) tali persone ed entità, compresi i fondi derivati o generati dai beni immobiliari di proprietà di o controllati direttamente o indirettamente da tali persone ed entità a loro collegate.

il terrorismo) definisce la misura in parola come il «*divieto di spostare, trasferire, alterare, utilizzare o trattare i capitali in modo da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura e la destinazione o da introdurre altri cambiamenti tali da consentire l'uso dei capitali in questione, compresa la gestione di portafoglio*».

Le misure di prevenzione patrimoniali previste dall'ordinamento italiano sono oggi disciplinate dal d.lgs. 159/2011 e consistono nel *sequestro di prevenzione* - nelle varianti *ordinaria* (art. 20), *anticipata* (art. 22, co. 1) ed *urgente* (art. 21, co. 2) - e nella *confisca* (art. 24).

Con particolare riferimento alla prevenzione del terrorismo, giova osservare che con il d.lgs. 22.6.2007, n. 109 (quindi anteriormente al *Codice Antimafia*)[338], il legislatore italiano ha introdotto - in attuazione della direttiva 2005/60/CE, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo - delle misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale.

In particolare, l'art. 1 del predetto decreto legislativo fornisce alcune rilevanti definizioni, tra le quali spiccano quelle di «*congelamento di fondi*» e di «*congelamento di risorse economiche*».

Il «*congelamento di fondi*» consiste nel «*divieto, in virtù dei regolamenti comunitari e dei decreti ministeriali di cui all'articolo 4, di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso dei fondi, compresa la gestione di portafoglio*» (art. 1, lett. e, d.lgs. 22.6.2007, n. 109).

---

[338]D.lgs. 22.6.2007, n. 109, recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE, è stato modificato dal d.lgs. 25.5.2017, n. 90, che ha attuato la direttiva 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Diversamente, per «*congelamento di risorse economiche*» si intende: «*il divieto, in virtù dei regolamenti comunitari e dei decreti ministeriali di cui all'articolo 4, di trasferimento, disposizione o, al fine di ottenere in qualsiasi modo fondi, beni o servizi, utilizzo delle risorse economiche, compresi, a titolo meramente esemplificativo, la vendita, la locazione, l'affitto o la costituzione di diritti reali di garanzia*» (art. 1, lett. f, d.lgs. 22.6.2007, n. 109)[339].

2. Il sistema delle fonti delle misure di prevenzione nell'ordinamento italiano

La disciplina delle misure di prevenzione nell'ordinamento repubblicano era inizialmente contenuta nella legge 27.12.1956, n. 1423, recante "*Misure di prevenzione nei confronti delle persone pericolose per la sicurezza e per la pubblica moralità*".

L'intervento normativo in parola, con l'intento di sottrarre le misure di prevenzione alla logica degli strumenti di polizia per reprimere le idee discordanti con quelle del regime fascista[340], ha ampliato notevolmente il novero dei destinatari delle stesse, ricomprendendovi - oltre agli oziosi ed ai vagabondi abituali - coloro i quali, sulla base di *elementi di fatto* o *notori*, dovessero ritenersi abitualmente dediti ai traffici delittuosi (art. 1, n. 1) o che, alla luce della loro

---

[339] Il d.lgs. 25.5.2017, n. 90 sostanzialmente riproduce il contenuto delle definizioni di congelamento di fondi e congelamento di risorse economiche fornite dall'art. 4, lettere e) ed f) del d.lgs. 22.6.2007, n. 109. Per un esame delle misure in parola si rinvia M. PELISSERO, *Reati contro la personalità dello Stato e contro l'ordine pubblico*, Giappichelli, 2010, pp. 163 e ss.; *Id.*, *Le "fattispecie di pericolosità": i presupposti di applicazione delle misure e le tipologie soggettive i destinatari della prevenzione praeter delictum: la pericolosità da prevenire e la pericolosità da punire*, in *Riv. It. Dir. Proc*., 2017, p. 439 e ss.; V. MAIELLO, *La legislazione penale in materia di criminalità organizzata, misure di prevenzione ed armi*, Giappichelli, 2015, p. 32 e ss.; A. NOCETI, M. PIERSIMONI, *Confisca e altre misure ablatorie patrimoniali*, Giappichelli, 2011, p. 91 e ss.

[340] Per un esame dell'evoluzione storica delle misure di prevenzione, con particolare attenzione per il loro impiego durante il fascismo, si rinvia a A. MANNA, *Misure di prevenzione e diritto penale: una relazione difficile*, IUS PISA, 2019, pp. 29 e ss. Durante il periodo fascista, le fonti disciplinanti le misure di prevenzione erano la l. 6.4.1926, n. 1848 ed il R.D. 18.6.1931, n. 773 (c.d. TULPS).

condotta e del loro tenore di vita, vivessero grazie ai proventi di attività delittuose (art. 1, n. 2) o che, infine, fossero dediti alla commissione di reati che offendono (o mettono in pericolo) l'integrità fisica e morale dei minorenni, la sanità, la sicurezza o la tranquillità pubblica (art. 1, n. 3).

La legge 1423 del 1956 è stata abrogata dal d.lgs. 6 settembre 2011, n. 159, intitolato "*Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia*" (c.d. *Codice Antimafia*), che, nel raccogliere organicamente le disposizioni per il contrasto delle associazioni di tipo *mafioso* e *terroristico*, ha riorganizzato la materia delle misure di prevenzione.

Il d.lgs. 159/2011 disciplina le misure di prevenzione personali nel Titolo I del Libro I e quelle patrimoniali nel Titolo II dello stesso. I successivi titoli sono dedicati, rispettivamente, all'amministrazione, gestione e destinazione dei beni sequestrati e confiscati (Titolo III), alla tutela dei terzi ed ai rapporti con le procedure concorsuali (Titolo IV) e, infine, alla disciplina degli effetti delle misure ed alla previsione delle sanzioni in caso di inosservanza delle stesse (Titolo V).

Le maggiori novità, rispetto al sistema previgente, si sono registrate in relazione ai presupposti soggettivi per l'applicazione delle misure di prevenzione e, quindi, in punto di *pericolosità sociale* e di *categorie di destinatari*, alcune delle quali, tuttavia, sono state successivamente dichiarate costituzionalmente illegittime dalla Consulta[341].

---

[341] Tra le novità più significative introdotte con il d.lgs. 159/2011 figura l'ampliamento della platea dei soggetti legittimati a proporre l'applicazione delle misure di prevenzione, che la legge 1423/1956 limitava al Questore della provincia in cui il proposto dimora. L'art. 5 del d.lgs. 159/2011 consente che la proposta possa provenire anche dal Procuratore Nazionale Antimafia, dal Procuratore della Repubblica presso il Tribunale del capoluogo di distretto ove dimora il destinatario e dal Direttore della DIA, sottraendola così al monopolio dell'Autorità amministrativa. Sul tema della legittimazione a proporre le misure di prevenzione si veda M. F. CORTESI, *Le "nuove" misure di prevenzione personali*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali,* op. cit., pp. 232 e ss.; V. MAIELLO, *Le misure di prevenzione dopo il c.d. codice antimafia. Aspetti sostanziali e procedurali – profili sostanziali: le misure di prevenzione personali*, in *Giur. It.*, 6/2015, pp. 1523-1528.

3. I presupposti soggettivi per l'applicazione delle misure di prevenzione: l'appartenenza del soggetto alle categorie "terroristiche" (art. 4 del d.lgs. 159 del 2011)

Il d.lgs. 159/2011 ha ulteriormente ampliato la platea delle categorie soggettive dei destinatari delle misure di prevenzione.

In particolare, l'art. 4 del Codice Antimafia, nella sua versione originaria, ricomprendeva (solo) 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 artt. 284, 285, 286, 306, 438, 439, 605 e 630 c.p., nonché alla commissione dei reati con finalità di terrorismo anche internazionale (art. 4, lett. d) e gli istigatori, i mandanti e i finanziatori dei predetti reati (art. 4, lett. h)[342].

In particolare, la previsione *ex* art. 4, lett. d) è rimasta sostanzialmente invariata sino ad oggi, salvo l'aggiunta di un'ulteriore categoria di atti (di cui successivamente si dirà), onde si rendono opportune alcune osservazioni[343].

Sul punto giova preliminarmente evidenziare che nel nostro ordinamento è ormai pacificamente ammessa la punibilità degli atti meramente preparatori del

---

[342] Per una disamina delle categorie soggettive dei destinatari previste dagli artt. 1 e 4 d.lgs. 159/2011, con particolare attenzione per la distinzione fra pericolosità generica e qualificata si rinvia a A. MARTINI, *Essere pericolosi,* op. cit., pp. 105-131. Per un esame della pericolosità qualificata terroristica, invece, si consiglia la lettura di M. SODDU, *Terrorismo, pericolosità sociale e recidiva*, Pacini Giuridica, 2016, p. 54-57. L'art. 4 d.lgs. 159/2011 fa riferimento alle categorie soggettive cosiddette di *pericolosità qualificata*, che, in quanto tali, si distinguono da quelle di cui all'art. 1, d.lgs. 159/2011 – dette di *pericolosità generica* – il quale riproduce, in modo sostanzialmente inalterato, l'elenco di destinatari già individuati dall'art. 1 della l. 1423/1956. Le lettere d) e h) del summenzionato art. 4 si riferiscono al settore della pericolosità qualificata del terrorismo. Infine, M. F. CORTESI, *Le misure di prevenzione personali applicate dall'autorità giudiziaria*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali*, op. cit., p. 260 e ss., in cui l'autore esamina il concetto di *pericolosità sociale qualificata* in relazione alle misure di prevenzione personali applicate dall'autorità giudiziaria.

[343] Per un esame delle categorie dei destinatari delle misure di prevenzione personali si rinvia a F. MAZZACUVA, *Le persone pericolose e le classi pericolose*, in S. FURFARO (a cura di), *Misure di prevenzione*, UTET, 2013, pp. 110 e ss.

delitto. Invero la giurisprudenza e la dottrina, come noto, sono concordi nel ritenere che possano configurare il tentativo punibile non soltanto gli atti già *esecutivi* del delitto, ma anche quelli *preparatori*, purché *idonei* e *diretti* in *modo non equivoco* alla commissione dello stesso (art. 56 c.p.)[344].

Tuttavia l'art. 4, lett. d) contempla il caso di *atti preparatori*, *diretti* alla commissione di reati con finalità di terrorismo, per i quali – ferma la loro *obiettiva rilevanza* - non si richiedono i requisiti dell'*idoneità* e della *non equivocità*. Purtuttavia per tali atti è prevista l'applicazione di misure aventi forza sostanzialmente equivalente a quella della pena (cioè le misure di prevenzione).

La limitazione della libertà personale in via preventiva è dunque ammessa (paradossalmente) in ragione di requisiti diversi e, complessivamente, meno stringenti di quelli richiesti per punire la forma tentata dei *delitti* con finalità di terrorismo, sebbene in entrambi i casi rilevino già i meri atti preparatori. Si può pertanto sostenere che la normativa attuale consenta di applicare misure di prevenzione sostanzialmente penali rispetto a comportamenti che si collocano in

---

[344] Per quanto riguarda la giurisprudenza, Cass. pen., Sez. II, sent. 13.3.2012, n. 12175, in cui i giudici affermano che: «*ai fini del tentativo punibile, assumono rilevanza penale non solo gli atti esecutivi veri e propri del delitto pianificato, ma anche quegli atti che, pur essendo classificabili come atti preparatori, tuttavia, per le circostanze concrete (di luogo, di tempo, di mezzi, ecc.) fanno fondatamente ritenere che l'azione - considerata come l'insieme dei suddetti atti - abbia la rilevante probabilità di conseguire l'obiettivo programmato e che l'agente si trovi ormai ad un punto di non ritorno dall'imminente progettato delitto, e che il medesimo sarà commesso»*. Per quanto attiene alla dottrina, invece, A. GIUDICI, *Tentativo e atti preparatori: una questione sempre aperta*, in *Dir. Pen. Cont*., 1.6.2012, p. 4, in cui l'autore evidenzia che, sebbene la giurisprudenza di legittimità ritenga che anche agli atti preparatori – connotati dai requisiti previsti dall'art. 56 c.p. – possano rilevare ai fini dell'integrazione del tentativo di delitto, in dottrina permangono dubbi circa la *idoneità*, la *direzione* e la *non equivocità* degli atti in questione, siccome cronologicamente collocati in una fase in cui tali criteri non sono agevolmente rilevabili, attesa la scarsa connotazione sotto il profilo oggettivo degli atti. Più precisamente gli atti preparatori potranno rilevare *ex* art. 56 c.p. quando, *«valutati unitariamente, abbiano l'astratta attitudine a produrre il delitto programmato*», con «*rilevante probabilità di conseguire l'obiettivo programmato*» per il soggetto agente. In altri termini, il meccanismo criminoso deve essere stato avviato, ormai ineluttabilmente, ed «*il soggetto agente si deve trovare ad un punto di non ritorno dall'evento delittuoso perfetto*». Inoltre cfr. T. PADOVANI, *Diritto penale*, op. cit., p. 324, in cui l'autore, evidenziando che la commissione del reato (doloso) è normalmente tripartita in *ideazione*, *preparazione* ed *esecuzione*, afferma che «*la fase puramente ideativa è sempre irrilevante (cogitationis poenam nemo patitur), mentre tra la preparazione e l'esecuzione si colloca il tentativo*».

una fase ben anteriore alla soglia del tentativo punibile, solo in ragione della loro *obiettiva rilevanza* e *direzione* a sovvertire lo Stato o a commettere reati terroristici[345].

Tanto premesso è evidente come la verifica della compatibilità di un siffatto assetto rispetto ai principi costituzionali postuli, indispensabilmente, che venga chiarito il significato del concetto della «*obiettiva rilevanza*», tuttora controverso in dottrina[346].

Sulla base di un'interpretazione di tipo letterale, potrebbe ritenersi che il concetto in parola si riferisca a *criteri oggettivi*, in base ai quali parametrare la rilevanza degli atti per applicare le misure di prevenzione.

Tuttavia il legislatore non fornisce un elenco tassativo di detti criteri, lasciando irrisolte le criticità che interessano l'art. 4 d.lgs. 159/2011 sotto il profilo della determinatezza, con ampi margini di discrezionalità all'Autorità giudiziaria chiamata ad applicare le misure.

Sul punto non è intervenuto nemmeno il decreto-legge 18.2.2015, n. 7 (c.d. *Decreto Antiterrorismo*), recante misure urgenti per il contrasto del terrorismo,

---

[345] Autorevole dottrina ha evidenziato la sussistenza di profili di criticità connessi agli atti preparatori svincolati dai criteri obiettivi e garantistici previsti dall'art. 56 c.p. – e in particolare da quelli della *idoneità* e *non equivocità* rispetto al delitto perfetto – previsti dalla versione originaria dell'art. 4, lett. d), d.lgs. 159/2011. Sul tema F. BRIZZI, *Il terrorismo internazionale*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali*, op. cit., p. 468, in cui l'autore evidenzia che: «Anche a prescindere dall'evidente incertezza interpretativa derivante dalla distinzione – notoriamente assi problematica – tra "atti preparatori" ed "atti esecutivi", vi è infatti il rischio che le misure di prevenzione colpiscano soltanto coloro i quali si limitano a compiere atti preparatori in vista della loro successiva partecipazione ad un conflitto in territorio estero, non anche coloro che, spingendosi oltre l'*iter criminis*, iniziano a dare esecuzione a quanto già programmato». In altri termini, il rischio che si correva, mantenendo inalterata l'originaria versione dell'art. 4, lett. d), d.lgs. 159/2011, era quello di ammettere l'applicazione di misure sostanzialmente equivalenti alla pena (cioè le misure di prevenzione) nel caso di atti preparatori privi dei requisiti dettati dall'art. 56 c.p., e di non intervenire con le misure di prevenzione in quello di atti che (parimenti privi dei requisiti suddetti) fossero già esecutivi del delitto. Tale paradosso è stato parzialmente risolto con la novella apportata alla disposizione in parola dalla l. 17.10.2017, n. 161, di cui appresso si dirà nel testo.

[346] A. MARTINI, *Essere pericolosi. Giudizi soggettivi e misure personali*, op. cit., p. 113-114, in cui l'autore, evidenziando le criticità connesse alla mancata previsione dell'*idoneità* degli atti *ex* art. 4, lett. d), d.lgs. 159/2011, ritiene che per risolvere la questione sia indispensabile ricercare la definizione di *obiettiva rilevanza*.

limitatosi ad aggiungere al testo dell'art. 4, lett. d), d.lgs. 159/2011 le parole «*ovvero a prendere parte ad un conflitto in territorio estero a sostegno di un'organizzazione che persegue le finalità terroristiche di cui all'art. 270-sexies c.p.*» [347]. La modifica ha comportato un ampliamento del perimetro applicativo delle misure di prevenzione sotto il profilo soggettivo, con l'obbiettivo di contrastare specificatamente il fenomeno dei *returning foreign fighters*, ovverosia coloro che fanno ritorno in patria, dopo periodi di addestramento presso gruppi terroristici in territori stranieri, al fine di attuare quanto appreso[348].

La dottrina, nella perdurante assenza di una definizione normativa - ha osservato che il concetto di *rilevanza ex* art. 4, lett. d, d.lgs. 159/2011 assume un significato di portata causale. Conseguentemente gli atti a cui si riferisce la disposizione, pur essendo *inidonei* a norma dell'art. 56 c.p., sono comunque obiettivamente dotati di una portata causale legata ad uno scopo futuro (che non si richiede venga conseguito)[349].

---

[347] Il d.l. 18.2.2015, n. 7, intitolato «*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 iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione*», è entrato in vigore il 20 febbraio 2015 e ha introdotto rilevanti fattispecie delittuose in materia di reati terroristici. Sugli effetti delle modifiche al *Codice Antimafia* apportate dal *Decreto Antiterrorismo* si veda A. BALSAMO, *Decreto Antiterrorismo e riforma del sistema delle misure di prevenzione*, in *Dir. Pen. Cont.*, 2.3.2015, p. 10, in cui l'autore, in relazione all'art. 4, lett. d), d.lgs. 159/2011, evidenzia «[…] notevoli difficoltà inevitabilmente connesse alla distinzione – notoriamente quanto mai incerta – tra atti preparatori e atti esecutivi». Tali difficoltà, secondo l'autore (che prende in considerazione la misura dell'espatrio), condurrebbero a risultati paradossali in relazione all'applicazione delle misure di prevenzione personali, che vengono così riassunti: «L'effetto, dopo il Decreto antiterrorismo, potrebbe essere paradossale: le misure di prevenzione, e il connesso divieto di espatrio, potrebbero infatti applicarsi a chi si limita ai primi preparativi per prendere parte ad un conflitto in territorio estero, ma non anche al soggetto che inizia ad attuare l'intento programmato, ed appare ormai in procinto di lasciare il territorio nazionale».

[348] Per un esame del fenomeno dei *foreign fighters* che fanno ritorno in patria dopo periodi di addestramento presso i gruppi terroristici di Iraq e Syria si rinvia a E. POKALOVA, *Returning Islamist Foreign Fighters. Threats and Challenges to the West*, Springer, 2019, pp. 11 e ss.

[349] Sul punto cfr. A. MARTINI, *Essere pericolosi. Giudizi soggettivi e misure personali*, op. cit., p. 114, ove l'autore, criticamente, aggiunge che: «In questa ricostruzione emerge un paradosso: privando il giudizio causale prognostico del parametro della idoneità come

Ad ogni buon conto, in tema di riforme, la l. 17.10.2017, n. 161, recante modifiche al codice delle leggi antimafia e delle misure di prevenzione, ha apportato rilevanti novità alla disposizione in esame.

L'intervento novellatore ha ampliato ulteriormente il catalogo dei possibili destinatari delle misure di prevenzione, ricomprendendo coloro che compiono *atti esecutivi* diretti a sovvertire l'ordinamento statale o alla commissione dei reati con finalità di terrorismo, anche internazionale[350].

La ricomprensione degli atti esecutivi dei delitti di terrorismo o di eversione entro il perimetro applicativo delle misure di prevenzione ha dunque consentito di mitigare il precedente assetto, che, come si è detto, si riferiva esclusivamente agli atti preparatori, i quali, tuttavia, *non sono stati espunti dalla norma*, continuando a rilevare a prescindere dai requisiti di *idoneità* e *non equivocità* con le problematiche già evidenziate.

Con ogni evidenza la nuova versione dell'art. 4, lett. d), d.lgs. 159/2011 comporta una notevole estensione dell'area applicativa delle misure di prevenzione in relazione al profilo oggettivo degli atti, la quale, astrattamente, viene ad essere sovrapponibile a quello della pena prevista per la forma tentata del delitto, del pari relativa ad atti preparatori ed esecutivi.

In altre parole, l'art. 4, lett. d), d.lgs. 159/2011 – ferma la distinzione ontologica intercorrente tra la pena e le misure di prevenzione - consente di applicare misure sostanzialmente penali ad atti preparatori o esecutivi di delitti con finalità di terrorismo, a prescindere dalla sussistenza di particolari requisiti garantistici e senza il previo accertamento della responsabilità penale in un

---

adeguatezza, non rimane altro che la mera direzione soggettiva degli atti: ovvero una pericolosità personale».

[350] L'ampliamento della platea dei soggetti ai quali applicare le misure di prevenzione contro il terrorismo (*ex* art. 4 del d.lgs. 159/2011), ricomprendendovi coloro che pongano in essere atti già esecutivi, era auspicata da autorevole dottrina. In particolare F. BRIZZI, *Il terrorismo internazionale*, in F. BRIZZI, *Il terrorismo internazionale*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali*, op. cit., p. 468, in cui l'autore sostiene: «[…] sarebbe auspicabile l'ampliamento dell'ambito di applicabilità delle misure di prevenzione anche a coloro che compiano *atti preparatori ovvero esecutivi diretti* alla commissione di un reato in materia di terrorismo, con il non trascurabile effetto di assegnare a queste misure un ruolo simmetrico a quello già sperimentato con successo nel contrasto alla criminalità mafiosa».

apposito processo, ovviando così alle difficoltà connesse alla ricerca ed alla formazione della prova.

Per quanto attiene all'art. 4, lett. h), d.lgs. 159/2011, invece, si osserva che esso consente di applicare le misure di prevenzione a coloro che abbiano *istigato* alla commissione di uno dei reati previsti nella lettera d) della stessa disposizione, a prescindere dall'accoglimento dell'istigazione e dalla commissione del reato.

La previsione in esame consente dunque di limitare la libertà personale dell'istigatore attraverso una "scorciatoia", dal momento che non è richiesto il previo accertamento in un apposito processo della responsabilità penale *per il delitto di istigazione a delinquere ex* art. 414 c.p., né il requisito della pubblicità che l'istigazione deve avere a norma del primo comma dell'articolo da ultimo richiamato.

Per quanto riguarda le categorie soggettive relative alle misure di prevenzione patrimoniali, l'art. 16 d.lgs. 159/2011 prevede che esse possono applicarsi non solo rispetto ai soggetti di cui all'art. 4, ma anche alle «*persone fisiche e giuridiche segnalate al Comitato per le sanzioni delle Nazioni Unite o ad altro organismo internazionale competente per disporre il congelamento di fondi o di risorse economiche, quando vi sono fondati elementi per ritenere che i fondi o le risorse possano essere dispersi, occultati o utilizzati per il finanziamento di organizzazioni o attività terroristiche, anche internazionali*»

Tale previsione, che conferma la centralità rivestita dalle misure di prevenzione - in particolare di tipo patrimoniale - nel contrasto dei delitti con finalità di terrorismo, impone di valutare la strumentalità dei fondi o delle risorse economiche oggetto di congelamento rispetto al finanziamento di organizzazioni o attività terroristiche, sulla base di non meglio precisati *fondati elementi*. Questi, alla luce delle considerazioni svolte in punto di *obiettiva rilevanza*, devono consistere in elementi di fatto, che facciano ritenere il collegamento teleologico

tra i fondi o le risorse da congelare ed il finanziamento delle attività o delle organizzazioni terroristiche[351].

3.1. La pericolosità sociale del prevenuto

L'appartenenza del prevenuto ad una delle categorie soggettive descritte dagli artt. 1, 4 e 16 del Codice antimafia, a cui si è fatto riferimento nel precedente paragrafo, non è requisito sufficiente per l'applicazione delle misure di prevenzione.

La Corte Costituzionale, infatti, ha chiarito che il giudice, attraverso un apposito giudizio, deve altresì accertare la sussistenza, in concreto, della *pericolosità sociale* in capo al prevenuto[352].

La Corte di Cassazione, concordemente, ha precisato che il riconoscimento al proposto della condizione di *pericolosità* – rilevante in ordine all'applicazione delle misure di prevenzione - presuppone, in primo luogo, l'inquadramento dello stesso in una delle categorie criminologiche tipizzate negli artt. 1 e 4 del d.lgs. 159/2011 e, in secondo luogo, una successiva «*fase prognostica in senso stretto*»,

---

[351] Come si ricorderà, ricercando la definizione del requisito che devono possedere gli atti *ex* art. 4, lett. d), d.lgs. 159/2011, si è detto che la «*rilevanza*» assume un significato di portata causale. Parimenti, pare potersi ritenere che la medesima connotazione causale debba interessare il requisito richiesto per i fondi e le risorse funzionali alla commissione dei reati di terrorismo, ai fini dell'applicazione delle misure di prevenzione patrimoniali. Per completezza si rinvia a A. MARTINI, *Essere pericolosi. Giudizi soggettivi e misure personali*, op. cit., p. 114.

[352] Sul punto C. Cost., sent. 27.2.2019, n. 24, in cui i giudici - riferendosi peculiarmente alla misura della sorveglianza speciale - hanno chiarito che: «[…] *oltre alla verifica della riconducibilità del soggetto a una delle categorie oggi elencate nell'art. 4 del d.lgs. n. 159 del 2011, l'applicazione della misura personale della sorveglianza speciale richiede un ulteriore e distinto presupposto, rappresentato dalla pericolosità di quel soggetto per la sicurezza pubblica, richiesto dall'art. 6, co. 1, del d.lgs. n. 159/2011*». La necessità, ai fini dell'applicazione delle misure di prevenzione personali, dell'ulteriore requisito soggettivo della pericolosità sociale del proposto, assume una funzione garantistica, dal momento che, ferma l'appartenenza ad una delle categorie astratte tipizzate dal legislatore, si richiede anche la dimostrazione della probabilità, concreta ed attuale, che il soggetto commetta un delitto.

consistente nella valutazione delle probabili future condotte della persona in chiave di offesa ai beni tutelati[353].

Ad ogni modo, il d.lgs. 159/2011 non fornisce una definizione di *pericolosità sociale*, alla quale viene dedicato l'art. 203 c.p.[354].

Tuttavia la disposizione in parola, collocata nel Titolo VIII del Libro I del codice penale, relativo alle misure di sicurezza, definisce il soggetto socialmente pericoloso come colui che - anche se non imputabile o non punibile – ha commesso un fatto previsto dalla legge come reato (art. 202 c.p.) ed è probabile che ne commetta di nuovi. L'art. 203 c.p., inoltre, dispone che la qualità di persona socialmente pericolosa debba desumersi dalle circostanze indicate dall'art. 133 c.p.

Orbene, ancorché le misure di sicurezza e quelle di prevenzione siano accomunate - per quanto riguarda i presupposti - dalla pericolosità, è evidente come l'unica definizione codicistica della stessa non possa valere *tout court* anche per le seconde. Infatti, la natura predelittuale delle misure di prevenzione, non ammette che il prevenuto abbia già commesso un reato, pena lo svilimento della *ratio* delle stesse.

---

[353] Cass. pen., Sez. I, sent. 14.06.2017, n. 54119. In motivazione gli Ermellini hanno affermato che il giudizio di *attualità* della *pericolosità sociale*, rilevante in relazione alle misure di prevenzione, non si basa esclusivamente sull'ordinaria prognosi della probabile e concreta reiterabilità di qualsivoglia condotta illecita – come invece previsto in via generale dall'art. 203 c.p. - ma presuppone la precedente inscrizione del soggetto in una delle categorie criminologiche tipizzate dal legislatore, richiedendo l'accertamento di tale specifica inclinazione del soggetto.

[354] La mancanza di una definizione normativa di *pericolosità sociale* perdura tutt'oggi. Nel corso del tempo, sono state formulate diverse teorie, specie in ambito sociologico e psicologico, per spiegare la natura della pericolosità sociale. Tra queste figura la *teoria antropologica*, secondo la quale l'anomalia che spinge a delinquere sarebbe di carattere psico-fisico. Secondo la *teoria sociologica*, invece, la pericolosità avrebbe il suo fondamento nell'ambiente che circonda il soggetto, rilevando fattori politici, storici, religiosi, sociali, burocratici, ecc. Ebbene, la rinuncia a criteri obiettivamente rilevanti in base ai quali valutare, in concreto, la sussistenza della pericolosità sociale del prevenuto, comporterebbe l'applicazione del tutto discrezionale delle misure di prevenzione, fondata, ad esempio, sulla fisiognomica. Sul punto A. MARTINI, *Essere pericolosi. Giudizi soggettivi e misure personali*, op. cit., pp. 1 e ss.; M. SODDU, *La valutazione criminologica della pericolosità sociale e della recidiva*, in *Brainfactor*, 14.7.2015, pp. 3 e ss.; F. ZANUSO, *L'emergente attualità di Cesare Lombroso*, in L. PICOTTI, F. ZANUSO (a cura di), *L'antropologia criminale di Cesare Lombroso dall'Ottocento al dibattito filosofico-penale contemporaneo*, Edizioni Scientifiche Italiane, 2011, p. 7.

La pericolosità richiesta per le misure di prevenzione, dunque, si differenzia sostanzialmente da quella descritta dall'art. 203 c.p., dal momento che non è necessariamente collegata all'affermazione della responsabilità per un fatto di reato[355]. Conseguentemente la valutazione circa la pericolosità del prevenuto non potrà basarsi esclusivamente sui criteri dettati dall'art. 133 c.p., relativi alla gravità del reato ed alla capacità di delinquere del colpevole. Diversamente, nel giudizio di pericolosità, il giudice dovrà esaminare l'intera personalità del soggetto, ricorrendo, se necessario, alle presunzioni, purché fondate su elementi obiettivi e su fatti specifici ed accertati[356].

La differenza intercorrente tra la pericolosità prevista dall'art. 203 c.p. e quella richiesta ai fini dell'applicazione delle misure di prevenzione è stata evidenziata anche dalla Corte di Cassazione. Secondo gli Ermellini, la seconda non si basa esclusivamente sull'ordinaria prognosi di probabile e concreta reiterabilità di qualsivoglia condotta illecita - come previsto in via generale dall'art. 203 c.p. - ma presuppone la precedente inscrizione del soggetto in una delle categorie criminologiche tipizzate dal legislatore nel Codice antimafia, richiedendo, pertanto, l'accertamento di tale specifica inclinazione del soggetto[357].

La Corte Costituzionale si è pronunciata più volte con riferimento al presupposto della *pericolosità* rilevante ai fini dell'applicazione delle misure di prevenzione e al relativo *giudizio*, ribadendo che essa deve essere accertata *in concreto* e connotata dal requisito dell'*attualità* nel caso delle misure personali[358].

---

[355] R. GUERRINI, L. MAZZA, S. RIONDATO, *Le misure di prevenzione. Profili sostanziali e processuali*, CEDAM, 2004, pp. 2 e ss., in cui gli autori spiegano che la pericolosità sociale, presupposto per l'applicazione delle misure di prevenzione, consiste più generalmente nell'*immoralità*, nella *predisposizione al delitto* o nella *presunzione di una condotta nelle relazioni umane dedita al delitto*, senza che, tuttavia, sia raggiunta alcuna prova di reità.

[356] P. PITTARO, *Misure di prevenzione personali e sistema penale*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali*, op. cit., p. 204 e ss.

[357] Cass. pen., Sez. I, sent. 14.06.2017, n. 54119.

[358] S. RECCHIONE, *La pericolosità sociale esiste ed è concreta: la giurisprudenza di merito resiste alla crisi di legalità generata dalla sentenza "De Tommaso v. Italia" (e confermata dalle sezioni unite "Paternò")*, commento a Trib. Roma, sez. spec. misure di prevenzione, decr. 3 aprile 2017, n. 30 (con memoria depositata dalla Procura della Repubblica di Tivoli) e a Trib.

La Corte ha altresì ritenuto costituzionalmente illegittimo un sistema che consenta di irrogare le misure di prevenzione sulla base di meri sospetti e presunzioni, come quello adottato dal legislatore fascista e sostanzialmente confermato dalla legge 1423/1956[359].

Per quanto attiene agli elementi da valutare ai fini dell'accertamento della pericolosità, essi consistono negli eventuali comportamenti antisociali o illeciti del prevenuto o, ancora, nei rapporti da questo intrattenuti con soggetti di cui sia già stata accertata la pericolosità. Nel giudizio di pericolosità potranno essere impiegati anche i criteri previsti dall'art. 133 c.p. e, in particolare, quelli del *carattere* (art. 133, co. 2, n. 1, c.p.) e dei *precedenti giudiziari* del reo, della *condotta* e della *vita* dello stesso (art. 133, co. 2, n. 2, c.p.), nonché delle sue *condizioni di vita individuale*, *familiare* e *sociale* (art. 133, co. 2, n. 4, c.p.). Con riferimento al giudizio di pericolosità, i summenzionati criteri potranno essere impiegati, al più, nell'ottica di ricostruire il quadro generale della personalità del reo e quindi compiere una prognosi criminale, volta a valutare la probabilità che egli commetta il reato[360].

Invero, come ha chiarito la Corte Costituzionale, il grado di certezza ed obbiettività richiesto ai fini del giudizio di prevenzione è collegato ad una *ragionevole prognosi*, coincidente con una *valutazione di «probabilità»* in ordine alla commissione, da parte del soggetto proposto, di illeciti penali. Tale valutazione prognostica deve poggiare su «*elementi di fatto*», i quali possono essere costituiti anche soltanto da riscontri indiziari, senza la necessità che rivestano la consistenza di «prove», dal momento che – attesa la *ratio*

Palermo, Sez. I – misure di prevenzione, decr. 1 giugno 2017, n. 62, in *Dir. Pen. Cont*., 10/2017, pp. 133 e ss.

[359] Già con la risalente sentenza 17.3.1969, n. 32, i giudici della Corte Costituzionale statuirono che la pericolosità di un soggetto non può essere desunta dalla mera appartenenza dello stesso ad una delle categorie tipizzate dal legislatore. Infatti, secondo quanto affermato dai giudici, occorre accertare la concreta sussistenza della pericolosità, da desumere attraverso un autonomo giudizio, che tenga conto di particolari elementi sintomatici connotati da *obiettiva rilevanza*.

[360] Sul punto A. MARTINI, *Essere pericolosi. Giudizi soggettivi e misure personali*, op. cit., pp. 170-186 e ss., in cui l'autore evidenzia la necessità che nel giudizio volto a valutare la pericolosità sociale del proposto vengano impiegati, in chiave prognostica, i criteri previsti dall'art. 133 c.p.

dell'intervento predelittuale - l'obiettivo non è pervenire ad una decisone penale che certifichi la «certezza» dell'avvenuta perpetrazione del fatto di reato[361].

In ogni caso gli *indizi* impiegati nella valutazione della *pericolosità* devono consistere in *elementi di fatto concreti* (non essendo invece sufficienti dei meri *sospetti*), dai quali sia possibile far discendere il giudizio probabilistico in ordine alla futura commissione di reati[362].

Con specifico riferimento al presupposto della pericolosità per l'applicazione delle misure di prevenzione patrimoniali, poi, giova evidenziare che l'art. 19, co. 1, d.lgs. 159/2011, rubricato "*Indagini patrimoniali*", prevede che l'autorità proponente, in ordine alla loro applicazione, compia delle indagini sul tenore di vita, sulle disponibilità finanziarie, sul patrimonio, sull'attività

---

[361] C. Cost., sent. 27.2.2019, n. 24. In motivazione i giudici, spiegando la distinzione esistente fra l'accertamento della responsabilità per la commissione di un fatto di reato (che deve fondarsi su riscontri probatori che permettano di superare ogni ragionevole dubbio) e la verifica "processuale" circa la *pericolosità sociale* del soggetto, definiscono quest'ultima come la «*rilevante probabilità di commissione, nel futuro, di ulteriori attività criminose*». Sul tema M. F. CORTESI, *Le misure di prevenzione personali applicate dall'autorità giudiziaria*, in AA.VV., F. FIORENTIN (a cura di), *Le misure di prevenzione personali e patrimoniali*, op. cit., p. 260 e ss., in cui l'autore afferma che: «Detto altrimenti, tale pericolosità (n.d.r. rilevante ai fini dell'applicazione delle misure di prevenzione) può essere definita come la ragionevole probabilità che la persona compia attività illecite o antisociali, così da rendere necessaria una risposta proporzionata ed efficace da parte dell'autorità». Nello stesso senso F. BRIZZI, P. PALAZZO, A. PERDUCA, *Le nuove misure di prevenzione personali e patrimoniali*, op. cit., pp. 22 e ss.; F. MENDITTO, *Presente e futuro delle misure di prevenzione (personali e patrimoniali): da misure di polizia a prevenzione della criminalità da profitto*, in *Dir. Pen. Cont*., 23.5.2016, p. 23.

[362] M. F. CORTESI, *Le misure di prevenzione personali applicate dall'autorità giudiziaria*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali*, op. cit., p. 262, in cui l'autore esamina il giudizio di pericolosità e precisa che questo: «si risolve in una prognosi sul futuro comportamento del soggetto desunto da elementi sintomatici, da ciò deriva che debba essere compiuto un esame complessivo della personalità del proposto, con una valutazione globale della condotta». Inoltre l'autore precisa che gli elementi sintomatici non possono consistere in meri sospetti, essendo invece necessari «fatti concreti ed elementi obiettivi aventi sicuro valore sintomatico». Nello stesso senso S. P. FRAGOLA, *Le misure di prevenzione*, CEDAM, 1992, pp. 17-23, che però aggiunge: «[…] è possibile enucleare alcuni parametri valutativi per l'accertamento in discorso sulla base di elementi antigiuridici ovvero riguardanti la morale genericamente intesa, elementi che possono prescindere da eventuali fatti di reato ma debbono comunque riguardare l'intera condotta di vita, tenuto conto di pregresse manifestazioni di pericolosità purché la pericolosità persista e, quindi, sia attuale»; F. MENDITTO, *Presente e futuro delle misure di prevenzione*, op. cit., p. 23. In giurisprudenza si registrano, conformemente, Cass. pen., Sez. VI, 6.2.2001, n. 12511 e Cass. pen, Sez. V, 11.7.2006, n. 40731.

economica e sulle fonti di reddito dei soggetti indicati al precedente art. 16 - a cui si è già fatto cenno - nei confronti dei quali possa essere proposta la misura di prevenzione della sorveglianza speciale della pubblica sicurezza, con o senza divieto od obbligo di soggiorno[363].

Con ogni evidenzia, le indagini patrimoniali sono finalizzate a stabilire se i redditi e, più in generale, la disponibilità economica del prevenuto siano compatibili con le sue attività lecitamente svolte o se, invece, sussistano squilibri che, unitamente agli altri parametri obiettivamente rilevanti, evidenzino la concreta pericolosità – sotto il profilo patrimoniale - del soggetto, nel senso della probabilità che egli, servendosi di quei fondi o risorse, possa commettere il reato.

Sempre in punto di pericolosità rilevante ai fini dell'applicazione delle misure di prevenzione patrimoniali, giova evidenziare che l'art. 18, co. 1, del d.lgs. 159/2011 consente la loro applicazione anche disgiuntamente dalle misure personali e, addirittura, indipendentemente dalla sussistenza - al tempo della richiesta - della pericolosità sociale del proposto. Tuttavia sarà in ogni caso necessario accertare che detta pericolosità sussistesse al tempo in cui il soggetto attinto dalla misura si era procurato i beni o le risorse direttamente interessate dalle misure[364].

L'art. 18, co. 3, d.lgs. 159/2011, invece, disciplina il diverso caso dell'applicazione delle misure di prevenzione patrimoniali nei confronti di soggetti in capo ai quali la pericolosità sociale non sussiste né al tempo della richiesta della misura né al tempo in cui essi hanno avuto la disponibilità dei beni o delle risorse finanziarie. Trattasi del caso della morte del soggetto in possesso

---

[363] Per un esame della fase delle *indagini patrimoniali*, con particolare attenzione per i titolari del potere d'indagine e per l'oggetto delle stesse, si rinvia a F. BRIZZI, *Indagini patrimoniali*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali*, op. cit., pp. 594 e ss.

[364] Sul presupposto della pericolosità per l'applicazione delle misure di prevenzione patrimoniali si veda G. GRASSO, *Le misure di prevenzione personali e patrimoniali nel sistema costituzionale*, in *Dir. Pen. Cont*., 14.2.2020, p. 2. Per una disamina sui presupposti applicativi delle misure di prevenzione patrimoniali, invece, A. BALSAMO, V. D'AGOSTINO, *Inquadramento sistematico ed evoluzione storica delle misure di prevenzione patrimoniali*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali*, op. cit., pp. 503 e ss.

dei requisiti previsti dall'art. 16 del d.lgs. 159/2011, che legittima l'applicazione delle misure nei riguardi dei suoi successori a titolo universale o particolare.

In altri termini la disposizione consente di applicare le misure di prevenzione patrimoniali sulla base della sola qualifica di successore di un soggetto pericoloso defunto, a prescindere dall'accertamento, in concreto, della sussistenza dei presupposti soggettivi previsti dal d.lgs. 159/2011, legittimando una forma di pericolosità che autorevole dottrina ha criticamente qualificato come *oggettiva*[365].

La giurisprudenza ha assunto posizioni discordanti in materia.

Le Sezioni Unite della Corte di Cassazione, con sentenza del 20 aprile 1995, hanno statuito che un bene (e dunque i fondi e le risorse finanziarie) non può essere, di per sé, né *pericoloso* né *utile* e che tali condizioni dipendono esclusivamente dalle mani in cui esso si trova, ribadendo che «*la criminosità e la pericolosità che impongono la confisca non costituiscono un carattere della cosa in sé, ma derivano dalla relazione fra questa e l'agente*»[366].

La Corte Costituzionale, invece, sul presupposto della diversa *ratio* che anima le misure di prevenzione personali e patrimoniali, ha sostenuto un orientamento diametralmente opposto rispetto a quello della Cassazione. Invero, secondo il giudice delle leggi, la funzione della confisca consiste nel sottrarre definitivamente un bene al circuito economico di origine connotato da condizionamenti criminali, al fine di inserirlo in un contesto lecito. Detta funzione caratterizza le misure patrimoniali, distinguendole da quelle personali e rendendole applicabili anche oltre la permanenza in vita del soggetto pericoloso[367].

---

[365] L. FILIPPI, M. F. CORTESI, *Il Codice delle misure di prevenzione*, Giappichelli, 2011, pp. 18-19, in cui gli autori osservano criticamente come l'art. 18, co. 3, d.lgs. 159/2011 sembri attribuire alla *res* - anziché al soggetto - la pericolosità, la quale, conseguentemente, potrà essere ritenuta sussistere in forza di mere presunzioni e, quindi, senza un accertamento in concreto, all'esito di un apposito giudizio, che tenga conto dei criteri obbiettivamente rilevanti di cui precedentemente si è fatto cenno.

[366] Cass., SS.UU., sent. 13.1.1995, n. 2.

[367] C. Cost., sent. 25.1.2012, n. 21.

3.2. Il giudizio di pericolosità

La sussistenza dei presupposti soggettivi per l'applicazione delle misure di prevenzione personali e, in particolare, della pericolosità sociale deve essere valutata in un apposito giudizio. Non esistono espresse previsioni normative che regolino il *giudizio di pericolosità*, la cui disciplina è frutto delle elaborazioni giurisprudenziali.

Invero, la Corte Costituzionale, già nella risalente sentenza n. 32 del 1969, chiariva che l'irrogazione delle misure di prevenzione presuppone di verificare che, in capo al prevenuto, sussista una condotta di vita tale da rivelare una pericolosità che deve possedere i connotati dell'*effettività* e dell'*attualità* e che, in ogni caso, non *deve essere meramente potenziale*[368].

In altri termini, per la valutazione della pericolosità sociale, il giudice è chiamato a prendere in considerazione gli elementi di fatto risultanti dalla valutazione complessiva di tutte le manifestazioni sociali del prevenuto, compresi gli eventuali comportamenti illeciti (anche non penali). La concretezza del giudizio in parola e i criteri sintomatici sui quali esso verte garantiscono il rispetto dei principi di materialità e di offensività, i quali, nella fase anteriore all'integrazione del tentativo punibile, postulano la predisposizione del prevenuto al delitto.

Ad ogni buon conto, la Corte di Cassazione ha descritto dettagliatamente le due fasi in cui si articola il giudizio di pericolosità.

La prima fase ha natura «*constatativa*» ed è finalizzata alla raccolta di tutti i dati idonei a dimostrare che il soggetto proposto ha tenuto una condotta contraria

---

[368] C. Cost., sent. 17.3.1969, n. 32. Nella sentenza (relativa alle misure questorili) i giudici, oltre ad indicare i requisiti che devono connotare la pericolosità, hanno altresì statuito che le norme contenute negli artt. 1 e 2 della l. 27.12.1956, n. 1423 - le quali conferiscono al Questore il potere discrezionale di adottare misure di prevenzione nei confronti delle persone pericolose per la sicurezza e per la pubblica moralità - non violano il principio della riserva di legge *ex* art. 13, co. 2, Cost. e sono quindi costituzionalmente legittime. Invero la discrezionalità di cui si avvale l'Autorità amministrativa nel giudizio di pericolosità - che non può ridursi al mero arbitrio - deve essere esercitata nell'ambito delle norme che la regolano e per il conseguimento dei fini voluti dalla legge. Tale discrezionalità è assoggettata al sindacato della competente Autorità giudiziaria.

alle ordinarie regole di convivenza. Più precisamene si può affermare che il primo momento del procedimento di pericolosità prevede lo svolgimento di un'attività essenzialmente *cognitiva*, tesa a conoscere tutto ciò che può essere utile al fine di valutare l'*antisocialità* (e, si badi, non la rilevanza penale) della condotta del prevenuto.

La seconda fase, invece, ha natura «*prognostica*» ed è volta a stabilire, sulla base degli elementi emersi nel corso della prima, se sia probabile che le condotte antisociali si ripetano[369].

In conclusione, si può osservare come il giudizio di pericolosità non sia finalizzato a stabilire se un soggetto sia responsabile per un determinato fatto di reato, bensì se egli sia pericoloso in rapporto al suo precedente agire, quale indice rivelatore della possibilità di commettere un reato in futuro. La pericolosità può rilevare quale presupposto per irrogare una misura di prevenzione solo qualora sia connotata da *attualità* e *concretezza*.

Con riguardo al primo requisito, esso potrebbe venire successivamente meno, con conseguenze diverse a seconda che il giudizio penda ancora o, invece, si sia già concluso con esito positivo ed applicazione della misura. Invero nel

---

[369] Cass. pen., Sez. VI, sent. 6.2.2001, n. 12511 e, conformemente, Cass. pen, Sez. V, sent. 11 luglio 2006, n. 40731. Gli ermellini hanno affermato che, ai fini dell'applicazione della misura di prevenzione della sorveglianza speciale di pubblica sicurezza con obbligo di soggiorno, non è sufficiente, per affermare la pericolosità del soggetto, un'unica intercettazione ambientale tra soggetti indiziati di appartenere ad un'associazione mafiosa, nel corso della quale si menzioni il prevenuto (in modo peraltro non rilevante ai fini dell'identificazione di elementi concreti di pericolosità a suo carico). Infatti gli elementi da considerare per l'applicazione delle misure di prevenzione - sebbene non necessitino dell'efficacia probatoria richiesta dal procedimento penale - devono raggiungere quantomeno la consistenza dell'indizio, non potendosi risolvere in meri sospetti, semplici congetture o illazioni. In dottrina V. MAIELLO, *Le misure di prevenzione dopo il c.d. Codice antimafia. Aspetti sostanziali e aspetti procedurali - profili sostanziali: le misure di prevenzione personali*, op. cit., pp. 1523-1528, in cui l'autore sostiene che: «La pericolosità del soggetto per la sicurezza pubblica attiene, invero, all'obbiettiva sussistenza di una pericolosità sociale effettiva, fondata su una base di fatto accertata giudizialmente, ed estrinsecantesi in una condotta antisociale protrattasi nel tempo da epoca precedente alla formulazione della proposta e fino al momento della pronuncia del decreto che chiude il procedimento di prevenzione. Deve trattarsi, quindi, di una pericolosità concreta, attuale, sussistente e accertata dal giudice. Il giudizio di pericolosità sociale può essere fondato su dati estratti da procedimenti penali anche pendenti, da precedenti penali e giudiziari e vanno valutati in maniera autonoma dal giudice della prevenzione».

primo caso il procedimento dovrebbe interrompersi mentre, nel secondo, ricorrerebbe un fondato motivo per chiedere la revoca del provvedimento da parte dell'Autorità che lo ha emanato, su istanza dell'interessato e sentita l'Autorità di pubblica sicurezza che lo ha proposto (art. 11, co. 2, d.lgs. 159/2011)[370].

4. *Le misure di prevenzione al vaglio della più recente giurisprudenza europea e domestica*

I numerosi profili di criticità che connotano le misure di prevenzione e la perdurante mancanza di un intervento del legislatore - che ne adegui finalmente la disciplina ai principi costituzionali - hanno suscitato, in tempi relativamente recenti, l'interesse della Grande Camera della Corte europea dei diritti dell'uomo[371].

I giudici di Strasburgo, con la sentenza 23.2.2017, De Tommaso c. Italia (ricorso 43395/09) - pronunciandosi in relazione a fatti anteriori al 2011 - hanno ritenuto che la disciplina delle misure di prevenzione prevista dalla l. 27.12.1956, n. 1423 (in larga parte oggi trasfusa nel Codice antimafia, al quale è quindi possibile estendere i ragionamenti della Corte), sebbene sia *accessibile* per l'interessato e dotata di *base legale*, non soddisfa i canoni qualitativi richiesti dalla Convenzione europea dei diritti dell'uomo in punto di *prevedibilità*. La carenza di tale requisito non interessa soltanto i presupposti applicativi delle misure, ma anche il contenuto delle stesse, tuttora affetto da grave indeterminatezza[372].

---

[370] S. FURFARO, *In tema di superamento delle presunzioni nel giudizio di prevenzione*, in *Giur. It*., 7/2013, p. 1655, in cui l'autore precisa che la misura di prevenzione si riferisce alla «*potenzialità offensiva*» del soggetto, saldamente unita alla «*attualità*» di tale pericolo.

[371] Per un esame dei profili di criticità che interessano la disciplina delle misure di prevenzione, S. RIONDATO, *Le misure di prevenzione e il degrado delle garanzie delle garanzie annunciato da Giuseppe Bettiol*, in AA.VV. (a cura di S. RIONDATO), *Dallo Stato Costituzionale Democratico di ritto allo Stato di polizia*, Padova University Press, 2012, pp. 117 e ss.

[372] Il testo della sentenza è disponibile nel sito del Ministero della Giustizia al link: *https://www.giustizia.it/giustizia/it/mg_1_20_1.page?facetNode_1=0_8_1_11&facetNode_2=1_2(*

A poca distanza dalla pronuncia della Corte europea, la Corte Costituzionale italiana è intervenuta in materia con la sentenza 27.2.2019, n. 24, che, in mancanza di un intervento legislativo adeguatore, ha dichiarato l'illegittimità dell'art. 1, lett. a), d.lgs. 159/2011, che consentiva di applicare le misure di prevenzione nei confronti di coloro che «*debbano ritenersi, sulla base di elementi di fatto, abitualmente dediti a traffici delittuosi*» (art. 1, lett. a, d.lgs. 159/2011)[373].

L'esame delle predette pronunce offre interessanti spunti per riflettere in ordine alla natura giuridica delle misure di prevenzione – che, è bene premetterlo sin d'ora, i giudici non ritengono incompatibili con i rispettivi ordinamenti – e ad una sistematica riforma della loro disciplina, che finalmente consenta di renderle pienamente conformi ai principi del diritto europeo ed a quelli costituzionali[374].

2017)&facetNode_3=1_2(201702)&facetNode_4=0_8_1_12&contentId=SDU1323549&previsio usPage=mg_1_20#.

[373] Il testo integrale della sentenza è disponibile presso il sito della Corte Costituzionale, al link: *https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2019&numero=24*.

[374] Sulla compatibilità delle misure di prevenzione con la Convenzione europea dei Diritti dell'Uomo, si veda F. MENDITTO, *La sentenza de Tommaso c. Italia: verso la piena modernizzazione e la compatibilità convenzionale del sistema della* prevenzione, in *Dir. Pen. Cont.*, 4/2017, p. 13, in cui l'autore spiega che: «La Corte ha più volte affermato la compatibilità con la Cedu di norme analoghe a quelle italiane, oltre che delle stesse misure di prevenzione, ritenute "limitative" e non "privative" della libertà personale, perciò compatibili con l'art. 2 del protocollo n. 4». Tra le sentenze più significative in cui la Corte europea dei Diritti dell'Uomo ha riconosciuto la compatibilità delle misure con i principi della Convenzione europea dei Diritti dell'Uomo, si rammentano C. EDU, 1.7.1961, *Lewless* c. Irlanda e C. EDU, 18.6.1971, *De Wilde* e altri c. Belgio. Per quanto attiene alla compatibilità delle misure di prevenzione e, più precisamente, della loro *ratio* rispetto all'ordinamento costituzionale italiano si veda G. GRASSO, *Le misure di prevenzione personali e patrimoniali nel sistema costituzionale*, op. cit., p. 4. In giurisprudenza C. Cost., sent. 5 maggio 1959, n. 27, in cui i giudici hanno affermato che: le misure di prevenzione «sono informate al principio di prevenzione e di sicurezza sociale, per il quale l'ordinato e pacifico svolgimento dei rapporti fra i cittadini deve essere garantito, oltre che dal sistema di norme repressive dei fatti illeciti, anche da un parallelo sistema di adeguate misure preventive contro il pericolo del loro verificarsi nell'avvenire. È questa un'esigenza e regola fondamentale di ogni ordinamento, accolta e riconosciuta dalla nostra Costituzione». Nello stesso senso D. PULITANÒ, *Relazione di sintesi. Misure di prevenzione e problema della prevenzione*, in *Riv. it. dir. proc. pen.*, 2017, p. 638 e ss.

4.1. La sentenza della Corte europea dei diritti dell'uomo del 23 febbraio 2017, De Tommaso c. Italia (ricorso n. 43395/09)

Il sig. Angelo De Tommaso adiva la Corte europea dei Diritti dell'Uomo con ricorso 28.7.2009, sostenendo che la misura della sorveglianza speciale di pubblica sicurezza, alla quale era stato sottoposto - per la durata di due anni e con le prescrizioni *ex* art. 5 della l. 1423/1956 - dal Tribunale di Bari con decreto 11.4.2008, violasse gli artt. 5, 6 e 13 CEDU e 2 del Protocollo n. 4 ad essa relativo[375]. Il Tribunale aveva irrogato la misura ritenendo la sussistenza di tutti i presupposti necessari e, peculiarmente, della pericolosità sociale del proposto. Questa era stata desunta sulla base dei precedenti penali del ricorrente per traffico di droga, evasione, possesso illegale di armi e delle sue frequentazioni con pregiudicati. Invero, secondo il giudice di primo grado, il De Tommaso (già sottoposto ad avviso orale in data 18.6.2006) non aveva migliorato la sua condotta ed, anzi, aveva continuato a frequentare esponenti di spicco della malavita e ad essere coinvolto in vari fatti criminosi, anche contro l'ordine e la sicurezza pubblici.

La Corte d'Appello di Bari, su ricorso del proposto, annullava la misura della sorveglianza speciale con decreto del 28.1.2009, ritenendo che non vi fosse la prova della sua pericolosità. In particolare, la Corte territoriale evidenziava che le più recenti attività illegali del De Tommaso, inerenti la droga, risalivano a più di cinque anni prima della richiesta della misura e che, comunque, egli non aveva violato gli obblighi della sorveglianza speciale. Infine, secondo la Corte territoriale, il Tribunale aveva omesso di valutare l'impatto riabilitativo che la pena, scontata dal proposto per i precedenti reati, aveva avuto sulla sua personalità.

---

[375] L. ROCCATAGLIATA, *Da Strasburgo: la misura di prevenzione della sorveglianza speciale di pubblica sicurezza viola al Convenzione EDU (Sentenza De Tommaso)*, in *Giur. Pen. web*, 24.2.2017 (disponibile in *https://www.giurisprudenzapenale.com/2017/02/24/strasburgo-la-misura-prevenzione-della-sorveglianza-speciale-pubblica-sicurezza-viola-la-convenzione-edu/*).

La Corte europea dei Diritti dell'Uomo ha dichiarato la disciplina italiana delle misure di prevenzione e, segnatamente, gli artt. 1, 3 e 5 della l. 1423/1956 (oggi parzialmente riprodotti negli artt. 1, 6 e 8 del d.lgs. n. 159/2011) in contrasto con l'art. 2 del Protocollo addizionale n. 4 CEDU (reso esecutivo in Italia con d.p.r. 217/1982).

La disposizione da ultimo richiamata sancisce la libertà delle persone di circolare nel territorio di uno Stato, di ivi fissare la propria residenza (art. 2, par. 1) e, in ogni caso, di lasciare in qualsiasi momento il Paese in cui si trovino (art. 2, par. 2).

L'art. 2, par. 3, dello stesso Protocollo, inoltre, ammette che le suddette libertà possano essere oggetto di restrizioni, purché queste ultime, da un lato, siano *previste dalla legge* e, dall'altro lato, costituiscano - in una società democratica - *misure necessarie* alla sicurezza nazionale ed a quella pubblica, al mantenimento dell'ordine pubblico, alla prevenzione delle infrazioni penali, alla protezione della salute, della morale, dei diritti e delle libertà altrui.

In particolare, per quanto attiene al requisito della *previsione per legge*, la Corte afferma la necessità che la restrizione abbia un'*adeguata base legale* nell'ordinamento nazionale (sia cioè «*in accordance with law*») e che presenti i requisiti dell'*accessibilità* («*accessibility*») e della *ragionevole prevedibilità* («*foreseeability*»). In altri termini, la disposizione che limita la libertà di circolazione deve essere agevolmente reperibile dai consociati e deve permettergli di conoscere, con anticipo, se ed in che misura la loro libertà di circolazione possa subire delle limitazioni, qualora essi si determinino a tenere un determinato comportamento.

Orbene, con riferimento al sistema italiano delle misure di prevenzione, la Corte europea dei diritti dell'uomo ha individuato la base legale delle restrizioni alla libertà di circolazione negli artt. 1, 3 e 5 della l. n. 1423/1956, ritenendo che essi soddisfino il requisito dell'*accessibilità*[376].

---

[376] L. DELLA RAGIONE, *Le misure di prevenzione nello specchio del volto costituzionale del sistema penale*, op. cit., p. 21; A. MANNA, *Misure di prevenzione e diritto penale: una relazione difficile*, op. cit., pp. 176 e ss.

Diversamente, osservano i giudici, le summenzionate disposizioni violerebbero il requisito della *prevedibilità*, mancante il quale le limitazioni del diritto alla libera circolazione delle persone non possono operare (art. 2, par. 3, del Protocollo addizionale n. 4 CEDU). In particolare, la Corte ha ritenuto che la carenza di prevedibilità sia dovuta allo scarso grado di precisione delle disposizioni della l. 1423/1956, tale da impedire ai cittadini di valutare le conseguenze delle loro azioni[377].

Invero, secondo i giudici, la previsione di una base legale (art. 2 del Protocollo 4 CEDU), connotata dai requisiti dell'*accessibilità* e soprattutto della *prevedibilità*, consente di limitare la discrezionalità dell'Autorità giudiziaria, che deve irrogare la misura di prevenzione all'esito del giudizio di pericolosità.

Sulla scorta delle suesposte ragioni, la Corte, in primo luogo, ha escluso che le misure di prevenzione possano adottarsi sulla base di un mero sospetto, postulando, invece, un oggettivo accertamento della pericolosità, da condurre in concreto. A tal uopo l'interprete deve prendere in considerazione elementi fattuali («*objective assessment of factual evidence*») rivelatori del comportamento abituale, dello stile di vita e, più in generale, dei comportamenti esteriori del soggetto, valutandone la rilevanza come manifestazione della tendenza a delinquere[378].

In secondo luogo, i giudici di Strasburgo hanno statuito che la legge 1423/1956 contrasta con i principi dettati dalla Convenzione europea dei diritti dell'uomo, perché non contiene previsioni sufficientemente dettagliate, che consentano di stabilire anzitempo se una condotta sia espressiva della pericolosità sociale. In particolare gli artt. 1 e 3 della l. 1423/1956 non consentono di individuare con precisione le categorie di persone alle quali sono applicabili le misure di prevenzione, impedendo ai consociati di prevedere se ed in quale misura la loro libertà personale potrà essere limitata per i comportamenti tenuti.

---

[377] P. PITTARO, *La natura giuridica delle misure di prevenzione*, in AA.VV., F. FIORENTIN (a cura di), *Le misure di prevenzione personali e patrimoniali*, op. cit., p. 163.

[378] G. GRASSO, *Le misure di prevenzione personali e patrimoniali nel sistema costituzionale*, op. cit., p. 6.

Infine, la Corte ha censurato anche la *vaghezza* e l'*imprecisione* delle disposizioni di cui al relativo art. 5, che prevede quali prescrizioni il Tribunale è tenuto ad indicare, in ogni caso, qualora disponga l'applicazione di una misura di prevenzione e, in particolare, quelle consistenti nel «*vivere onestamente*» e nel «*rispettare le leggi*». Invero, a parere dei giudici europei, tali prescrizioni si sostanziano in un «illimitato richiamo all'intero ordinamento giuridico italiano» che «non fornisce alcuna chiarificazione sulle norme specifiche la cui inosservanza dovrebbe essere considerata quale ulteriore indicazione del pericolo per la società rappresentato dall'interessato». La stessa disposizione è stata censurata anche nella parte in cui consente all'Autorità giudiziaria di «imporre tutte quelle prescrizioni che ravvisi necessarie, avuto riguardo alle esigenze di difesa sociale; ed in particolare, il divieto di soggiorno in uno o più comuni, o in una o più Province». Essa, infatti, riconosce un illimitato potere discrezionale al giudice chiamato ad applicare la misure di prevenzione, dal momento che, di tali prescrizioni, la legge non determina alcun contenuto specifico[379].

4.2. Osservazioni critiche sulla sentenza De Tommaso

La sentenza De Tommaso offre alcuni interessanti spunti di riflessione per valutare la compatibilità dell'attuale disciplina italiana delle misure di prevenzione (prevista dal d.lgs. 159/11) rispetto ai principi del diritto eurounitario ed a quelli costituzionali.

Una prima questione attiene alle libertà di *circolazione*, di *fissazione della residenza* e di *lasciare lo Stato* in cui ci si trovi, previste dall'art. 2 del Protocollo 4 CEDU, con le quali, secondo i giudici, la disciplina italiana delle misure di prevenzione contrasta.

---

[379] Per completezza si segnala che la Corte ha censurato anche l'art. 5 della l. n. 1423/1956, nella parte in cui impedisce di «partecipare a pubbliche riunioni». Al riguardo, sostengono i giudici, la legge non prevede alcun limite di spazio o di tempo a questa libertà fondamentale, la cui restrizione viene quindi lasciata interamente alla discrezionalità del giudice.

In proposito giova osservare che le censure della Corte europea, in punto di indeterminatezza e carenza di prevedibilità della disciplina italiana, avrebbero dovuto, a rigor di logica, indurre i giudici ad assumere, quale parametro per valutarne la compatibilità rispetto al diritto europeo, l'art. 5 CEDU. Infatti la previsione in parola, nel sancire l'inviolabilità della sicurezza e della libertà personale - che è il bene giuridico direttamente attinto dalle misure di prevenzione personali - indica i casi eccezionali in cui essa può essere limitata (art. 5, par. 1)[380]. Tra questi l'art. 5, par. 1, lett. a) prevede la regolare detenzione a seguito della condanna del Tribunale, mentre l'art, 5, par. 1, lett. c) riferisce il caso dell'arresto o della detenzione (con traduzione innanzi all'Autorità giudiziaria) di un soggetto, quando ricorrano motivi plausibili di sospettare che egli abbia commesso un reato o che possa commetterlo o, ancora, che possa fuggire dopo averlo commesso.

Tuttavia se, da un lato, il riferimento all'art. 5 CEDU avrebbe certamente reso il ragionamento della Corte più logico e coerente con la sua decisione finale, dall'altro lato, esso avrebbe comportato il *formale riconoscimento* della natura penale delle misure di prevenzione, con l'applicazione delle garanzie di cui agli artt. 6 e 7 CEDU e conseguenze potenzialmente dirompenti per l'ordinamento italiano.

---

[380] L'art. 5, par. 1, CEDU, nel sancire l'inviolabilità della libertà e della sicurezza, indica i casi eccezionali in cui la persona può essere privata della libertà: (a) se è detenuto regolarmente in seguito a condanna da parte di un tribunale competente; (b) se si trova in regolare stato di arresto o di detenzione per violazione di un provvedimento emesso, conformemente alla legge, da un tribunale o allo scopo di garantire l'esecuzione di un obbligo prescritto dalla legge; (c) se è stato arrestato o detenuto per essere tradotto dinanzi all'autorità giudiziaria competente, quando vi sono motivi plausibili di sospettare che egli abbia commesso un reato o vi sono motivi fondati di ritenere che sia necessario impedirgli di commettere un reato o di darsi alla fuga dopo averlo commesso; (d) se si tratta della detenzione regolare di un minore decisa allo scopo di sorvegliare la sua educazione oppure della sua detenzione regolare al fine di tradurlo dinanzi all'autorità competente; (e) se si tratta della detenzione regolare di una persona suscettibile di propagare una malattia contagiosa, di un alienato, di un alcolizzato, di un tossicomane o di un vagabondo; (f) se si tratta dell'arresto o della detenzione regolari di una persona per impedirle di entrare illegalmente nel territorio, oppure di una persona contro la quale è in corso un procedimento d'espulsione o d'estradizione.

Ad ogni buon conto, sebbene la Corte europea dei diritti dell'uomo abbia scelto - quasi con rispettoso timore - di non pronunciarsi con riguardo alla natura formale delle misure di prevenzione, ha comunque ritenuto, quantomeno indirettamente, che esse siano strumenti sostanzialmente penali.

Invero, i giudici, in relazione alla necessità che le restrizioni della libertà di circolazione previste dall'art. 2, par. 3, del Protocollo n. 4 CEDU abbiano una base legale, hanno affermato che quest'ultima deve presentare i caratteri dell'*accessibilità* e della *prevedibilità*. Più precisamene l'intervento che i giudici europei ritengono necessario per adeguare la disciplina italiana delle misure di prevenzione ai principi eurounitari è la *tassativizzazione dei parametri* che consentono ai consociati di stabilire se ed in che misura la loro libertà possa essere limitata, in ragione dei comportamenti tenuti. Ebbene, tali presupposti, a ben guardare, rappresentano l'essenza dello stesso *principio di legalità* e del suo *corollario della determinatezza* (art. 25 Cost.), che orientano il diritto penale costituzionale.

Conclusivamente si possono svolgere alcune osservazioni.

La maggioranza dei giudici della Corte, come precedentemente cennato, ha respinto la prospettazione del ricorrente secondo cui le misure di prevenzione – ed in particolare la sorveglianza speciale - sarebbero da considerare (formalmente) delle pene, ritenendole non equiparabili alle sanzioni penali, dal momento che il procedimento che conduce alla loro applicazione non comporta la valutazione su un'accusa penale[381].

Tale impostazione è senz'altro condivisibile, atteso che, come si è già detto, la pena è strumento che interviene per definizione *post delictum* e comunque all'esito di un procedimento che abbia accertato la penale responsabilità del reo, con funzione eminentemente retributiva[382]. Diversamente, le misure di prevenzione sono impiegate *ante delictum*, per evitare, in chiave special-preventiva, la commissione del reato da parte del destinatario delle stesse.

---

[381] In questi termini si esprimono i giudici al paragrafo §. 143 della sentenza in esame.

[382] M. RONCO, *Il significato retributivo-rieducativo della pena*, in *Dir. Pen. e Proc*., 2005, pp. 137 e ss.

La pronuncia della Corte evidenzia che, pur dovendosi rifiutare una formale qualificazione delle misure di prevenzione alla stregua di pena, esse devono comunque essere sottoposte ad una disciplina che offra adeguate garanzie ai prevenuti, quantomeno sotto il profilo del principio di legalità e dei suoi corollari della determinatezza e della tassatività.

Una siffatta posizione potrebbe essere valorizzata per sostenere la natura sostanzialmente penale delle misure di prevenzione[383] o, quantomeno – secondo una diversa prospettazione che si ritiene di condividere - la necessità che degli strumenti tanto pervasivi, tali da limitare la libertà personale del destinatario (senza che sia stato commesso un reato e senza un equo processo) siano sottoposte a garanzie analoghe a quelle che interessano la pena[384].

---

[383] L. DELLA RAGIONE, *Le misure di prevenzione nello specchio del volto costituzionale del sistema penale*, op. cit., p. 37, in cui l'autore sostiene condivisibilmente che: «In una prospettiva più generale è necessario ricondurre la disciplina delle misure di prevenzione alla *matière pénale* così da consentire l'applicazione delle necessarie garanzie al di là delle etichette utilizzate (senza vergogna) dal legislatore nazionale». L'autore aggiunge che, in accordo alle argomentazioni dei giudici di Strasburgo, alle misure di prevenzione debbano estendersi le garanzie penalistiche - peculiarmente quelle sancite dall'art. 25 Cost. - conformemente a quanto già sostenuto dagli stessi nella sentenza *Grande Stevens*. In quel caso si era ritenuto che il concetto di *pericolosità* fosse da ricondurre alla materia penale, con conseguente applicazione - al giudizio per il suo accertamento ed alle misure che da essa dipendono – dell'apparato di garanzie previste dagli artt. 6 e 7 CEDU

[384] A completamento dell'esame della decisione in commento, pare interessante evidenziare quanto sostenuto criticamente da alcuni commentatori. In particolare, si veda P. PITTARO, *Misure di prevenzione personali e sistema penale*, in AA.VV., F. FIORENTIN (a cura di), *Le misure di prevenzione*, op. cit., p. 163, in cui l'autore sostiene che la sentenza De Tommaso non avrebbe prodotto effetti dirompenti rispetto alla disciplina italiana delle misure di prevenzione. Invero, sotto un primo profilo, i giudici europei non hanno risolto la questione della natura delle misure di prevenzione, limitandosi a negare che esse, ed in particolare la sorveglianza speciale, siano equiparabili ad una sanzione penale. Sotto un diverso profilo, invece, i giudici hanno attribuito centralità al requisito della *prevedibilità*, il quale, di fatto, consente di superare la questione della natura delle misure di prevenzione. Queste, a prescindere dalla loro riconducibilità alla sfera penale o amministrativa, potranno sempre applicarsi, purché la restrizione del diritto sia di volta in volta prevedibile da parte del proposto.

4.3. La sentenza 24 gennaio 2019, n. 24 della Corte Costituzionale: il dialogo "mediato" tra la Corte europea e quella nazionale

Con la sentenza 24.1.2019, n. 24, la Consulta si è pronunciata sulla legittimità costituzionale degli artt. 1, 3 e 5 della l. 1423/1956, dell'art. 19 della l. 152/1975 e degli artt. 1, 4, co. 1, lett. c), 6 e 8 del d.lgs. 159/2011, in riferimento all'art. 117, co. 1, Cost., in relazione all'art. 2 del IV Protocollo CEDU[385].

In particolare, la Corte Costituzionale ha dichiarato l'illegittimità costituzionale dell'art. 1, lett. a), d.lgs. 159/2011 (già art. 1, n. 1, l. 1423/1956), che consentiva di applicare le misure di prevenzione – e in particolare la sorveglianza speciale - nei confronti di coloro che «*debbano ritenersi, sulla base di elementi di fatto, abitualmente dediti ai traffici delittuosi*», censurando l'indeterminatezza della previsione rispetto agli artt. 13 e 117, co. 1, Cost., in riferimento all'art. 2, Prot. 4 CEDU. Diversamente, i giudici hanno affermato la legittimità costituzionale della disposizione *ex* art. 1, lett. b), d.lgs. 159/2011 (già art. 1, n. 2, l. 1423/1956), ritenendola sufficientemente precisa.

La questione è stata sollevata in un contesto giuridico assai delicato, segnato, da un lato, dalla sentenza De Tommaso della Corte europea dei Diritti dell'Uomo di quasi due anni prima e, dall'altro lato, dalla perdurante inerzia del legislatore italiano, convitato di pietra che nulla aveva fatto nel predetto biennio per adeguare il sistema delle misure di prevenzione ai principi del diritto eurounitario.

La Corte Costituzionale ha preliminarmente osservato che le misure di prevenzione, ancorché rappresentino il lascito - sostanzialmente immutato per oltre un secolo - di una produzione normativa di polizia ottocentesca rivolta a

---

[385] La questione di legittimità costituzionale è stata sollevata dalla Corte d'Appello di Napoli con ordinanza del 15.3.2017, n. 154. Per completezza si segnala che, contestualmente, la Corte territoriale ha interrogato la Consulta anche circa la legittimità costituzionale del solo art. 19 della l. 152/1975, in riferimento all'art. 117, co. 1, Cost., in relazione agli artt. 1 del Protocollo addizionale CEDU firmato a Parigi il 20.3.1952 e 42 Cost. Successivamente anche il Tribunale di Udine e quello di Padova hanno promosso giudizi di legittimità aventi ad oggetto le stesse norme, rispettivamente con ordinanze 10.4.2017, n. 115 e 30.5.2017, n. 146.

soggetti posti ai margini della società (vagabondi, oziosi, sospettati per furti di campagna, ecc.), non sono incompatibili con i principi costituzionali[386].

Secondo i giudici, la *ratio* di impedire o, quantomeno, rendere più difficoltosa la commissione di reati da parte di un determinato soggetto può giustificare la compressione della sua libertà personale. Infatti lo scopo delle misure di prevenzione è «*il controllo, per il futuro, della pericolosità sociale del soggetto interessato*» e non invece «*la punizione per ciò che questi ha compiuto nel passato*»[387]. Tali considerazioni dei giudici Costituzionali, consentono di rilevare che la *ratio* delle misure di prevenzione esula dalle funzioni general-preventiva e retributiva (proprie della pena) e, pur avendo un connotato special-preventivo, si rivolge specificamente al concetto di pericolosità.

Tuttavia i giudici hanno riconosciuto che gli strumenti in parola incidono profondamente sulla *libertà personale ex* art. 13 Cost. e che pertanto essi devono rispettare le condizioni dettate da tale disposizione ed i requisiti di *legalità*, *accessibilità* e *prevedibilità* sanciti dalla Corte europea dei Diritti dell'Uomo nella sentenza De Tommaso[388].

---

[386] La Corte Costituzionale ha affermato la compatibilità delle misure di prevenzione con i principi della Costituzione sin dalla sentenza 5 maggio 1959, n. 27, rilevando che esse: «sono informate al principio di prevenzione e di sicurezza sociale, per il quale l'ordinato e pacifico svolgimento dei rapporti fra i cittadini deve essere garantito, oltre che dal sistema di norme repressive dei fatti illeciti, anche da un parallelo sistema di adeguate misure preventive contro il pericolo del loro verificarsi nell'avvenire. È questa un'esigenza e regola fondamentale di ogni ordinamento, accolta e riconosciuta dalla nostra Costituzione».

[387] C. Cost., sent. 24.1.2019, n. 24, §. 9.7.1.

[388] *Ibidem*, in cui si legge che: «La stessa Corte EDU, nella recente sentenza che – come si dirà più innanzi – è all'origine delle presenti questioni di legittimità costituzionale, ha espressamente escluso che le misure di prevenzione personali sottoposte al suo esame costituiscano sanzioni di *natura sostanzialmente punitiva* [il corsivo è mio], come tali soggette ai vincoli che la Convenzione detta in relazione alla materia penale (Corte EDU, sentenza 23 febbraio 2017, de Tommaso contro Italia, paragrafo §. 143). Né la Corte Costituzionale, nelle varie occasioni in cui ha sinora avuto modo di pronunciarsi sulle misure di prevenzione personali, ha mai ritenuto che esse soggiacciano ai principi dettati, in materia di diritto e di processo penale, dagli artt. 25, co. 2, 27, 111, terzo, quarto e quinto comma, e 112, Cost.». Tuttavia, ad essere precisi, nella sentenza De Tommaso (§. 32) l'atteggiamento dei giudici europei è più prudente di come descritto dalla Consulta. Essi infatti non si pronunciano, in modo espresso, sulla natura delle misure di prevenzione ed affermano che, ai fini dell'applicazione delle garanzie che il diritto europeo prevede per la materia penale (in particolare a norma dell'art. 6 CEDU), non è possibile

Le condizioni appena riferite concorrono a comporre un complesso sistema di garanzie, ancor *più stringente rispetto a quello tratteggiato dalla giurisprudenza europea*, che i giudici della Consulta hanno descritto nella motivazione della sentenza.

In primo luogo, le misure di prevenzione devono essere dotate di un'*idonea base legale*. In altri termini, anche gli strumenti in parola sono soggetti al *principio di legalità* ed in particolare alla *riserva di legge* (art. 25 Cost.). Quanto all'*idoneità*, poi, essa si riferisce alla determinatezza che deve connotare la base legale delle misure, ai fini della conoscibilità e prevedibilità da parte dei consociati, concorrendo, in ultima analisi, alla *certezza del diritto*.

In secondo luogo, tra le misure di prevenzione e i legittimi obiettivi di prevenzione dei reati, deve intercorrere un rapporto di stretta *proporzionalità*, che, come ha precisato la Corte, «*è requisito di sistema nell'ordinamento costituzionale italiano, in relazione a ogni atto dell'autorità suscettibile di incidere sui diritti fondamentali dell'individuo*»[389].

In terzo luogo, la Corte ha affermato che le misure di prevenzione devono essere assoggettate alla *riserva di giurisdizione*. Tale requisito rappresenta il tratto emblematico del sistema di tutele costituzionalmente orientato, essendo del tutto inedito rispetto al complesso di garanzie delineato dai giudici europei nella sentenza De Tommaso. Invero, questi ultimi, riconducendo gli effetti delle misure di prevenzione alla violazione della libertà di circolazione (art. 2 del IV Protocollo

---

basarsi sulla qualificazione formale di «reato» e di «pena» offerta dai singoli ordinamenti nazionali. Diversamente, secondo i giudici europei, bisogna adottare un criterio sostanziale, cosicché le suddette garanzie dovranno applicarsi ogniqualvolta per un certo fatto sia prevista l'applicazione di misure che - a causa della loro natura o del grado di severità - siano comunque da ricondurre alla sfera penale. Tanto premesso, *non pare pienamente condivisibile* l'assunto della Corte Costituzionale che nega la natura sostanzialmente penale delle misure di prevenzione – le quali incidono pesantemente sulla libertà personale del destinatario – e l'applicazione delle garanzie tipicamente penali alle stesse. E infatti la necessità, ravvisata dalla Consulta nella stessa sentenza, di applicare le misure di prevenzione nel rispetto dei principi di *riserva di legge*, *prevedibilità*, *accessibilità* e *riserva di giurisdizione* pare contraddire l'impostazione appena criticata.

[389] C. Cost., sent. 24.1.2019, n. 24, §. 9.7.3.

CEDU) - anziché a quella della libertà personale (art. 5 CEDU) - avevano ritenuto il requisito della riserva di giurisdizione (artt. 6 e 7 CEDU) superfluo[390].

Nell'elaborare i tre criteri appena enucleati, la Corte Costituzionale non si è spinta a qualificare espressamente la natura delle misure di prevenzione, limitandosi ad escludere la loro riconducibilità alla materia penale, quantomeno in senso formale. Tuttavia, allo stesso tempo, i giudici hanno ritenuto che agli strumenti in questione, sotto il profilo sostanziale, debbano essere applicate *garanzie*, che sono tipicamente penali, quali il *principio di legalità*, il *corollario della determinatezza*, la *riserva di legge*, il *principio della proporzionalità della pena*, nonché la *riserva di giurisdizione*.

Dette garanzie hanno una duplice funzione.

Esse, da un lato, consentono di sottrarre alla discrezionalità dell'Autorità amministrativa l'applicazione delle misure di prevenzione, evitando arbitrarie limitazioni della libertà personale.

Dall'altro lato, esse assicurano ai consociati di poter prevedere se e, eventualmente, in quale misura il comportamento che hanno tenuto potrà comportare una compressione della loro libertà personale in funzione preventiva, colmando la lacuna di prevedibilità censurata dalla Corte europea.

Nella seconda parte della sentenza, la Corte si è interrogata sulla possibilità di rendere costituzionalmente conformi le disposizioni sottoposte al suo vaglio e, nel caso, su quale strumento impiegare a tal fine.

Sul punto la Consulta, facendo leva sull'incerta natura degli strumenti in questione – che non è formalmente penale - e ferma la necessità che gli stessi si fondino su una base legale accessibile, ha ritenuto che la lacuna in punto di prevedibilità possa essere adeguatamente colmata, attraverso una *lettura*

---

[390] *Ibidem*. A ben vedere pare potersi affermare che è proprio il requisito della riserva di giurisdizione a rendere più stringente il sistema di garanzie costituzionali rispetto a quelle richieste dalla Corte europea, sottraendo le misure di prevenzione al monopolio dell'Autorità amministrativa ed imponendo che la loro applicazione consegua ad un apposito procedimento, assistito dalle garanzie del giusto processo penale e peculiarmente dal contraddittorio delle parti e dal diritto di difesa.

tassativizzante costituzionalmente orientata, senza la necessità di un intervento del legislatore, altrimenti indispensabile in materia penale[391].

Tuttavia la Corte ha precisato che il correttivo ermeneutico non può operare indistintamente rispetto a qualsiasi disposizione normativa, ammettendone l'operatività esclusivamente in relazione alle norme che presentino un grado di imprecisione che sia soltanto *lieve*. Diversamente l'interpretazione giurisprudenziale non è sufficiente rispetto alle norme che siano connotate da un deficit di determinatezza e imprevedibilità incolmabile, tali da costituire un «*guscio vuoto, bisognoso di arricchimenti contenutistici*», che solo l'intervento del legislatore può assicurare[392].

Il limite posto dalla Corte ha la funzione di scongiurare il rischio, insito nella pratica ermeneutica appena descritta, di legittimare il ruolo creativo della giurisprudenza, la quale, al più, può spiegare il significato della norma, onde chiarirne la collocazione entro il perimetro costituzionale[393].

Sulla base di questa distinzione, la Consulta, chiamata a pronunciarsi sulle categorie di soggetti destinatari delle misure di prevenzione previste dall'art. 1 della l. 1423/1956, è giunta a conclusioni diverse, ritenendo costituzionalmente legittima la previsione di cui al numero 2 della norma (ora art. 1, lett. b, d.lgs.

---

[391] Sul punto i giudici, al §. 12 della sentenza in commento, affermano che: «Tuttavia, allorché si versi al di fuori della materia penale, non può del tutto escludersi che l'esigenza di predeterminazione delle condizioni in presenza delle quali può legittimamente limitarsi un diritto costituzionalmente e convenzionalmente protetto possa essere soddisfatta anche sulla base dell'interpretazione, fornita da una giurisprudenza costante e uniforme, di disposizioni legislative pure caratterizzate dall'uso di clausole generali, o comunque da formule connotate in origine da un certo grado di imprecisione».

[392] G. GRASSO, *Le misure di prevenzione personali e patrimoniali nel sistema costituzionale*, op. cit., p. 12.

[393] L. DELLA RAGIONE, *Le misure di prevenzione nello specchio del volto costituzionale del sistema penale*, op. cit., p. 35, in cui l'autore evidenzia che l'interpretazione tassativizzante può infatti apparire per parte della dottrina un «atto di usurpazione della giurisprudenza che si sostituisce al compito disatteso colpevolmente dal legislatore, con pregiudizio per il modello orizzontale di separazione dei poteri». Nello stesso senso F. PALAZZO, *Per un ripensamento radicale del sistema di prevenzione ante delictum*, in *Discrimen*, 12.9.2018, pp. 12 e ss.

159/2011), ma non anche quella di cui al precedente numero 1 (ora art. 1, lett. a, d.lgs. 159/2011).

Secondo il ragionamento della Consulta è possibile assicurare contorni sufficientemente precisi alla fattispecie prevista dall'art. 1, n. 2, l. 1423/1956 - in modo da consentire ai consociati di prevedere se ed in quale misura la loro libertà potrà subire limitazioni in ragione dei comportamenti tenuti – attraverso un'*interpretazione tassativizzante*, che spieghi il significato del concetto di «*attività delittuose*»[394]. Tuttavia la Corte ritiene che tale percorso ermeneutico non possa limitarsi ad una sterile elencazione di *titoli di reato* - secondo il rigido schema del *numerus clausus* - che difficilmente potrà essere esaustiva, preferendo optare per l'elaborazione dei criteri che identifichino la *categoria* dei delitti-presupposto, dai quali far dipendere l'applicazione delle misure di prevenzione[395].

Tali delitti devono essere: a) *commessi abitualmente*; b) *aver generato profitti in capo al proposto*; c) costituire – o aver costituito in una determinata epoca – l'unico reddito del soggetto, o quantomeno una componente significativa dello stesso[396].

---

[394] C. Cost, sent. 24.1.2019, n. 24, §. 12.2, in cui la Corte Costituzionale ha avuto cura di puntualizzare come: «[…] alla luce dell'evoluzione giurisprudenziale successiva alla sentenza De Tommaso, risulti oggi possibile assicurare in via interpretativa contorni sufficientemente precisi alla fattispecie descritta dell'art. 1, numero 2), della legge n. 1423 del 1956, poi confluita nell'art. 1, lettera b), del d.lgs. n. 159 del 2011, sì da consentire ai consociati di prevedere ragionevolmente in anticipo in quali "casi" – oltre che in quali "modi" – essi potranno essere sottoposti alla misura di prevenzione della sorveglianza speciale, nonché alle misure di prevenzione patrimoniali del sequestro e della confisca».

[395] L. DELLA RAGIONE, *Le misure di prevenzione nello specchio del volto costituzionale del sistema penale*, op. cit., p. 41, in cui si legge: «Il sufficiente grado di precisione emerge, secondo la Corte, nella predeterminazione non tanto di singoli "titoli" di reato, quanto di specifiche "categorie di reato"».

[396] C. Cost, sent. 24.1.2019, n. 24, §. 12.2. Le *categorie* dei reati-presupposto, individuate attraverso le tre caratteristiche che devono connotare gli stessi, valgono per l'applicazione sia delle *misure personali* sia di quelle *patrimoniali*. Tuttavia nell'uno e nell'altro caso è necessario che ricorrano ulteriori requisiti specifici. Quanto alle *misure di prevenzione personali* (in particolare quella della sorveglianza speciale, con o senza obbligo o divieto di soggiorno), al riscontro processuale dei tre requisiti elaborati dalla Consulta dovrà naturalmente aggiungersi la valutazione dell'effettiva pericolosità del soggetto per la sicurezza pubblica (art. 6, co. 1, del d.lgs. n. 159 del 2011). Quanto alle *misure di prevenzione patrimoniali* (in particolare quelle del sequestro e della confisca), invece, i requisiti di matrice giurisprudenziale dovranno «*essere accertati in relazione al*

Ad ogni buon conto, giova osservare che la scelta di prediligere un meccanismo interpretativo che tassativizzi le caratteristiche che devono accomunare i delitti (appartenenti ad una certa categoria) idonei a giustificare la limitazione della libertà personale in via preventiva - anziché i singoli titoli di reato - produce *nuovi doveri in capo al giudice*. Questo, infatti, qualora ritenga di irrogare una misura di prevenzione ad uno dei soggetti individuati dall'art. 1, lett. b) della d.lgs. 159/2011, non potrà più limitarsi ad accertare la sussistenza dei requisiti soggettivi e oggettivi dettati dalla legge e precedentemente esaminati. Infatti egli dovrà altresì verificare che, in concreto, il proposto abbia posto in essere un delitto connotato dalle tre caratteristiche individuate dalla Corte Costituzionale.

La Consulta è pervenuta a conclusioni diverse con riguardo all'art. 1, n. 1, della l. 1423/1956 (confluita nell'art. 1, lett. a, d.lgs. 159/2011), che, fra i destinatari delle misure di prevenzione, annoverava «*coloro che debba ritenersi, sulla base di elementi di fatto, che sono abitualmente dediti a traffici delittuosi*».

La disposizione era costituzionalmente illegittima, siccome affetta da radicale imprecisione, che non poteva essere emendata con la sola interpretazione giurisprudenziale costituzionalmente conforme. Invero, essa abbisognava di un radicale intervento legislativo, che ne integrasse il contenuto troppo impreciso ed indeterminato, peculiarmente con riguardo al concetto di «*traffici delittuosi*». Secondo la Corte, tale termine era geneticamente vago e non ulteriormente specificato dal legislatore, tanto da impedire al giudice ed ai consociati di selezionare quali atti potessero costituire il presupposto per applicare le misure di prevenzione[397].

---

lasso temporale nel quale si è verificato, nel passato, l'illecito incremento patrimoniale che la confisca intende neutralizzare». Con riguardo alla relazione fra il suddetto lasso temporale e la provenienza del bene, si veda Cass., SS.UU., sent. 2.2.2015, n. 4880, in cui i giudici hanno affermato che la necessità della correlazione temporale in parola «discende dall'apprezzamento dello stesso presupposto giustificativo della confisca di prevenzione, ossia dalla ragionevole presunzione che il bene sia stato acquistato con i proventi di attività illecita».

[397] C. Cost., sent. 24.1.2019, n. 19, §. 13, in cui i giudici affermano: «Da ciò consegue l'illegittimità costituzionale, in ragione del loro contrasto con i parametri appena indicati, di tutte le disposizioni cui si riferiscono le questioni ritenute ammissibili (indicate al precedente punto 7),

Autorevole dottrina ha espresso un giudizio severamente negativo rispetto all'attuale sistema delle misure di prevenzione, nonostante gli effetti del correttivo tassativizzante della giurisprudenza.

Invero, le ipotesi di pericolosità qualificata resterebbero affette da un grave deficit di tassatività, legittimando la limitazione della libertà personale sulla base di presupposti, che - in mancanza di un intervento del legislatore - rischiano di rimanere dei sospetti scarsamente connotati sotto il profilo oggettivo[398]. Per tali ragioni pare condivisibile la posizione di chi ritiene opportuno ricondurre la disciplina delle misure di prevenzione alla *matière pénale*[399], superando il rigido formalismo con il quale il legislatore nazionale qualifica la pena e adottando una prospettiva sostanzialista, al fine di applicare le garanzie penali anche alle misure che limitano la libertà personale, a prescindere dalla commissione di un reato e senza un previo processo fondato su prove, quali sono le misure di prevenzione negativa[400].

---

nella parte in cui consentono di applicare le misure di prevenzione della sorveglianza speciale, con o senza obbligo o divieto di soggiorno, del sequestro e della confisca, ai soggetti indicati nell'art. 1, n. 1), della legge n. 1423 del 1956, poi confluito nell'art. 1, lett. a), del d.lgs. n. 159 del 2011, restando assorbita la questione relativa all'art. 25, co. 3, Cost.».

[398] Sul punto si pensi al concetto di *obiettiva rilevanza* degli *atti preparatori* dei delitti terroristici, di cui si è offerta un'interpretazione nel paragrafo §.4 di questo Capitolo.

[399] M. FATTORE, *Così lontani così vicini: il diritto penale e le misure di prevenzione Osservazioni su Corte EDU, Grande Camera, 23 febbraio 2017, De Tommaso c. Italia*, in *Dir. Pen. Cont*., 4/2017, pp. 97 e ss., in cui l'autore sostiene convintamente che le misure di prevenzione abbiano natura penale sia sotto il profilo sostanziale sia sotto quello formale: «Le misure di prevenzione sono sanzioni criminali e tutto il sistema prevenzionale è materia penale – tant'è che viene censurato dalla Grande Camera per mancanza di determinatezza, una delle tante facce del prisma della Legalità. […] Pur in un momento storico nel quale il concetto di sanzione ha smarrito i connotati tradizionali, possiamo serenamente affermare che la materia prevenzionale è penale sia su un piano sostanziale sia su quello sistematico».

[400] Con riferimento al giudizio negativo circa il sistema delle misure di prevenzione appena suesposto G. GRASSO, *Le misure di prevenzione personali e patrimoniali nel sistema costituzionale*, op. cit., p. 31. L'autore sostiene la necessità di estendere alle misure di prevenzione, delle quali riconosce la natura sostanzialmente penale, tutte le garanzie previste in questa materia, compreso il principio di irretroattività, che né la Corte europea dei Diritti dell'Uomo né la Corte Costituzionale hanno menzionato nelle rispettive motivazioni. Inoltre cfr. F. SIRACUSANO, *La tassativizzazione delle fattispecie di pericolosità per la sicurezza pubblica tra paradigmi convenzionali e garanzie costituzionali*, in *Arch. Pen*., 1/2022, p. 10, in cui l'autore evidenzia che il correttivo tassativizzante elaborato dalla giurisprudenza della Corte Costituzionale

5. Le misure di prevenzione contro le condotte con finalità cyberterroristiche

L'esame del sistema multilivello europeo delle fonti in materia di cibernetica (Convenzione di Budapest del 23.1.2001 e regolamento 2019/881) e, in particolare, di sistemi informativi (direttiva 2013/40 e direttiva 2016/1148), infrastrutture critiche (direttiva 2008/114/CE) e terrorismo *online* (regolamento 2021/784 e direttiva 2017/541), condotto nel precedente Capitolo di questo lavoro, ha evidenziato che sono *cyberterroristiche* - benché il legislatore sovranazionale non usi questo termine – le condotte che, servendosi dei sistemi informativi e di *Internet* come mezzi (variante *tool oriented* parzialmente disciplinata sia a livello nazionale che europeo) oppure rivolgendosi ai sistemi informativi nazionali e, più in generale, alle infrastrutture critiche cibernetiche come oggetti materiali (variante *target oriented* non disciplinata), possono arrecare – per la natura e il contesto - grave danno ad un Paese o ad un'organizzazione internazionale e sono comunque poste in essere allo scopo di intimidire la popolazione o costringere i poteri pubblici od 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.

C'è di più. Le potenzialità del *cyberspace*, da un lato, e la ricerca del significato dei concetti di *natura* e *contesto*, quali componenti essenziali dell'elemento oggettivo dei reati terroristici *ex* art. 1 della decisione quadro 2002/475/GAI - da sempre sottovalutati, se non addirittura ignorati, da parte della dottrina italiana impegnatasi nell'esegesi dell'art. 270-*sexies* c.p. –, dall'altro lato, confermano l'inadeguatezza delle vecchie fattispecie tipizzate a livello europeo e, a cascata, nazionale in materia di terrorismo.

---

produce l'effetto di estendere alle misure di prevenzione le garanzie previste per la materia penale, precisando che: la tassativizzazione è «orientata a confermare la necessaria presenza dei principi di garanzia del sistema penale per l'applicazione delle misure di prevenzione e dell'imprescindibile rispetto del principio di determinatezza della fattispecie come presupposto della prevedibilità dell'intervento giudiziale».

Infatti le condotte di terrorismo cibernetico si differenziano da quelle di terrorismo comune perché, oltre agli scopi *ex* artt. 1 della decisione quadro 2002/475/GAI e 270-*sexies* c.p., possono essere compiute, come si è detto, per perseguire un ulteriore fine[401].

Trattasi del *condizionamento delle scelte politiche dei cittadini di un Paese*, che può attuarsi avvalendosi di *Internet*, delle reti e dei sistemi informativi e, più in generale, di tutti i mezzi di comunicazione cibernetica – primi fra tutti i *social networks* – che, ad oggi, non ha ricevuto tipizzazione né a livello europeo né nazionale.

Tale ulteriore scopo, pur presentando innegabilmente dei legami con gli scopi terroristici già tipizzati, è autonomo rispetto ad essi, perché, senza la necessità dell'intimidazione diretta per la popolazione, presuppone un *condizionamento della libertà morale dei cittadini*, colpendo una delle forme più autentiche di manifestazione della stessa, ovverosia la libertà di scelta politica. Tale condizionamento, per altro verso, viene posto in essere mediante l'intromissione nel metodo democratico dello Stato, destabilizzandone le strutture politiche fondamentali.

Secondo la prospettiva eurounitaria, come si e detto nel precedente Capitolo di questo lavoro, la strategia da adottare per contrastare il *cybercrime* ed il cyberterrorismo deve essere improntata alla *prevenzione*. Tuttavia questa, diversamente dalle scelte compiute a livello nazionale, non può essere perseguita attraverso l'incontrollata proliferazione di nuove fattispecie (di repressione preventiva[402]), contraddistinte dall'anticipazione della soglia della rilevanza penale ad ogni costo, persino a quello di sacrificare i principi del diritto penale democratico.

È opportuno avvalersi, invece, di strumenti già noti all'ordinamento italiano, ovverosia le *misure di prevenzione*, che - diversamente dalla pena - consentono di intervenire nella fase *ante delictum*. Tuttavia l'applicazione degli

---

[401] In proposito si veda il §. 5. del Capitolo I di questo lavoro.

[402] L. PASCULLI, *Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali*, op. cit., pp. 83 e ss.

strumenti in parola può avvenire esclusivamente sulla base di rigorosi presupposti oggettivi e soggettivi, tra i quali figura l'accertamento della pericolosità sociale del proposto e la sua appartenenza ad una delle categorie previste dal *Codice antimafia*[403]. Sul punto la giurisprudenza europea e quella domestica hanno recentemente denunciato la carenza di *determinatezza* e *prevedibilità* che affligge la disciplina delle misure di prevenzione - peculiarmente l'art. 4 del d.lgs. 159/2011 - individuando in via interpretativa (attesa la perdurante inerzia del legislatore) gli ulteriori presupposti necessari a conformarla al *principio di legalità*, al *corollario di determinatezza* e, più in generale, al *principio della certezza del diritto*. L'accurata tassativizzazione dei requisiti applicativi delle misure di prevenzione consente ai consociati di prevedere, a fronte degli atti compiuti, se e quali restrizioni potrà subire la loro libertà già in fase predelittuale[404].

Ebbene, l'esigenza di determinatezza e prevedibilità si fa ancor più forte in un settore, come quello del crimine cibernetico, contraddistinto dal *cyberspace*, le cui caratteristiche - che rendono difficile se non impossibile un suo inquadramento entro le categorie tradizionali del diritto penale - si sono già esaminate in precedenza.

Per tali ragioni, ferma la compatibilità con l'ordinamento italiano della *ratio* delle misure di prevenzione[405], è opportuno procedere, *de iure condendo*, ad una tassativizzazione - che non sia solo frutto dell'interpretazione

---

[403] Sulla preferibilità delle misure di prevenzione, rispetto alle fattispecie penali prevenzionistiche, in ordine al perseguimento della funzione special-preventiva in M. RONCO, A. BERARDI, *Le pene principali*, in AA.VV., M. RONCO (a cura di), *Persone e sanzioni*, Zanichelli, 2010, pp. 280-281; M. RONCO, *Appunti di diritto penale*, op. cit., p. 248.

[404] F. SIRACUSANO, *La tassativizzazione delle fattispecie di pericolosità per la sicurezza pubblica tra paradigmi convenzionali e garanzie costituzionali*, op. cit., p. 10, in cui l'autore precisa che la tassativizzazione in parola è «orientata a confermare la necessaria presenza dei principi di garanzia del sistema penale per l'applicazione delle misure di prevenzione e dell'imprescindibile rispetto del principio di determinatezza della fattispecie come presupposto della prevedibilità dell'intervento giudiziale».

[405] Sul punto C. Cost., sent. 5.5.1959, n. 27, cit. Nello stesso senso, in dottrina, D. PULITANÒ, *Relazione di sintesi. Misure di prevenzione e problema della prevenzione,* op. cit., p. 638 e ss.

giurisprudenziale - dei presupposti per l'applicazione delle misure *ante delictum* contro il cyberterrorismo, attesa la specificità delle indicazioni europee in materia.

Ad ogni modo la determinazione dei presupposti per l'irrogazione delle misure di prevenzione dedicate al contrasto del fenomeno in parola può offrire, al legislatore italiano, lo spunto per valutarne di nuove, con peculiare attenzione per le *misure di prevenzione positiva* (c.d. *positive prevention*) – come caldeggiato a livello europeo - già ampiamente diffuse nei Paesi di *common law*, la cui *ratio* ed essenza ben si attagliano alla natura politica dei reati di cyberterrorismo (specie nel caso dello scopo del condizionamento delle scelte politiche dei consociati), nonché alle componenti oggettive della *natura* e del *contesto* dello stesso[406].

5.1. I presupposti soggettivi delle misure di prevenzione per il contrasto del cyberterrorismo

La disamina dell'attuale disciplina italiana delle misure di prevenzione e dei correttivi di cui essa abbisogna ha evidenziato che la sua costituzionalità dipende, in larga misura, da un sistema di presupposti soggettivi adeguatamente determinati, tali da permettere ai consociati di prevedere le conseguenze dei loro comportamenti.

Detti presupposti, che, come si è detto, consistono nelle *categorie dei destinatari* (astrattamente individuate dalla legge) e nella *pericolosità sociale*, assumono, con riferimento agli atti preparatori obiettivamente rilevanti per la commissione del cyberterrorismo, un'accresciuta qualificazione rispetto ai presupposti soggettivi *ex* art. 4, lett. d) e h), d.lgs. 159/2011, in ragione delle caratteristiche dello spazio cibernetico[407].

---

[406] Sulla compatibilità del fine di condizionamento delle scelte politiche rispetto ai reati politici si veda S. PANAGIA, *Il delitto politico nel sistema penale italiano*, CEDAM, 1980, pp. 90 e ss.; sul concetto di violenza politica A. SENALDI, X. CHIARAMONTE, *Violenza politica*, Ledizioni, 2018, pp. 7-16.

[407] Il nostro ordinamento, come si è visto, distingue due tipologie di pericolosità sociale: da un alto la *pericolosità generica* (art. 1, d.lgs. 159/2011) e, dall'altro lato, la *pericolosità*

5.1.1. La categoria dei destinatari delle misure di prevenzione contro il cyberterrorismo

Con riferimento alla categoria di destinatari rilevante per l'irrogazione delle misure di prevenzione contro il cyberterrorismo, è in primo luogo indispensabile interrogarsi sull'applicabilità, in generale, delle misure di prevenzione a coloro che intendano compiere atti preparatori obiettivamente rilevanti rispetto al reato in parola. Trattasi di un quesito solo apparentemente banale, che presuppone la piena comprensione della *natura del reato* in questione e dell'*interesse giuridico* che esso offende. Ebbene, non v'è dubbio che le misure di prevenzione possano essere impiegate anche in materia di cyberterrorismo, dal momento che questo è un reato politico, connotato dalle finalità previste dall'art. 270-*sexies* c.p. (oltre alla particolare finalità del condizionamento delle scelte politiche degli utenti-cittadini) e da una particolare gravità, in ragione dei beni giuridici offesi.

In secondo luogo, si ripropongono – acuendosi - le difficoltà connesse alla definizione del concetto di «*atti preparatori, obiettivamente rilevanti, diretti* […] *alla commissione di reati*», in questo caso con finalità di cyberterrorismo, peculiarmente in relazione allo scopo del *condizionamento delle scelte politiche dei cittadini di uno Stato* attraverso l'utilizzo abusivo dei sistemi cibernetici.

In effetti la natura del *cyberspace* - depersonalizzato, privo delle coordinate spazio-temporali tradizionali e svincolato dalla realtà materiale - rende assai difficile accertare i requisiti oggettivi richiesti dall'art. 4, lett. d) del d.lgs. 159/2011, imponendo di chiarire la distinzione intercorrente tra questi e gli atti

---

qualificata (art. 4, d.lgs. 159/2011). Il grado di maggior qualificazione è legato alle specifiche categorie di reato rispetto alle quali gli atti, contemplati dalla seconda disposizione, si riferiscono. Nel caso delle categorie *ex* art. 4, lett. d) e h), come noto, gli atti devono essere *obiettivamente rilevanti* rispetto ai reati terroristici. Orbene, le categorie soggettive che si riferiscono ai reati *cyberterroristici* sono ulteriormente qualificate (rispetto alle altre), in ragione delle peculiarità del *cyberspace*, il quale - come si è detto - presenta, tra i profili di maggiore criticità, una marcata depersonalizzazione. Tale aspetto rende difficile l'accertamento della pericolosità per irrogare le misure di prevenzione attraverso le categorie tradizionali di cui all'art. 4, postulandone di nuove, che tengano conto delle criticità predette.

rilevanti a norma dell'art. 56 c.p. (sempre in relazione al terrorismo cibernetico), onde scongiurare un duplice rischio.

Da un lato bisogna evitare che l'Autorità giudiziaria applichi arbitrariamente le misure di prevenzione, impiegandole per limitare la libertà dell'imputato - con effetti sostanzialmente analoghi alla pena - anche quando non sia agevole la prova della sua responsabilità (specie per il tentativo del delitto *ex* art. 56 c.p., attese le suesposte criticità). Inoltre, in tema di condizionamento delle scelte politiche dei cittadini, l'interprete potrebbe ritenere preparatori ed obiettivamente rilevanti atti che, in concreto, non lo sono. In proposito si pensi, ad esempio, al caso di legittime attività di pubblicazione di contenuti, che - pur riferendosi a posizioni o idee estremistiche - restano confinati in una fase anteriore a quella preparatoria del reato, senza obiettiva rilevanza per la sua commissione e, comunque, assolutamente privi, sotto il profilo soggettivo, dalla finalità cyberterroristica.

Dall'altro lato, la scarsa determinatezza della categoria *ex* art. 4, lett. d), d.lgs. 159/2011, in relazione al cyberterrorismo, interessa anche i consociati, che non riescono a prevedere se ed in quale misura la loro libertà personale o il loro patrimonio possano subire delle limitazioni per i comportamenti tenuti - magari per fini lavorativi, commerciali, pubblicitari, informativi o scientifici - nell'*Internet* e nei *social networks*.

Per tali ragioni sarebbe quindi opportuno procedere ad una dettagliata opera di tassativizzazione, mediante un intervento legislativo *ex novo* (attese le lacune in materia), che, facendo tesoro degli insegnamenti delle Corti europea e nazionale, renda superfluo un correttivo interpretativo a posteriori.

In particolare, secondo quanto è emerso dall'esame della sentenza n. 24/2019 della Consulta, la tassativizzazione non deve avere ad oggetto i singoli *titoli di reato*, pena la realizzazione di una sterile elencazione che non potrebbe essere esaustiva e creerebbe "zone grigie", tali da legittimare le scelte discrezionali dell'autorità giudiziaria. Differentemente l'intervento del legislatore deve avere ad oggetto *categorie di reati*, dettagliando le caratteristiche dei

comportamenti, che - valutati in concreto - giustificano l'applicazione delle misure di prevenzione, a prescindere dallo specifico titolo di reato.

5.1.2. La "pericolosità sociale cibernetica" ed i criteri per il suo accertamento nell'apposito giudizio

Maggiori difficoltà, proprio a causa delle succitate criticità del cyberspazio, emergono in relazione all'individuazione della *pericolosità sociale* rilevante per l'irrogazione delle misure di prevenzione del cyberterrorismo.

In proposito parrebbe opportuno introdurre il nuovo concetto di *pericolosità sociale cibernetica* (legata da un rapporto di specialità rispetto a quella generale), da accertarsi in concreto sulla base di criteri che l'interprete deve valutare nel corso di un apposito giudizio.

Questi, tenuto conto del peculiare scopo consistente nel condizionamento delle scelte politiche dei cittadini di uno Stato attraverso l'uso abusivo degli strumenti cibernetici di comunicazione, attengono precipuamente ai comportamenti tenuti dagli utenti nel loro utilizzo.

Il funzionamento dei *social networks* offre un'esemplificazione pratica.

L'utente di tali piattaforme, come noto, può comunicare riservatamente con altri utenti attraverso gli appositi sistemi di messaggistica (ad esempio *Messenger* per *Facebook* e i *Direct* per *Instagram*) oppure può effettuare delle pubblicazioni dal contenuto più vario (si pensi ai cosiddetti *posts*, alle foto, ai video, agli audio e alle *stories*). Dette pubblicazioni possono essere indirizzate ad un numero potenzialmente indeterminato di persone – impostando la *privacy* in pubblica - o, viceversa, rivolgersi a gruppi di soggetti più ristretti, magari accomunati dai medesimi interessi o caratteristiche, modulando le impostazioni della *privacy*. Ebbene, si può pertanto ritenere che il primo criterio da impiegare per valutare la pericolosità sociale cibernetica sia rappresentato dal *modo che il proposto adotta per comunicare nel cyberspace*, con particolare attenzione per il *contenuto* delle pubblicazioni e per i loro *destinatari*.

Altro criterio che rileva ai fini della valutazione del comportamento del proposto nel cyberspazio è il *modo di relazionarsi virtualmente con gli altri utenti*. Sul punto si dovrà tenere conto della rete di *amici*, *followers* e *followings* del soggetto, valutando le condotte poste in essere dagli stessi nel *cyberspace* e anche fuori di esso. Parimenti rilevanti sono le pagine seguite e, più in generale, i siti frequentati, specie se dedicati a contenuti estremistici, violenti o espressamente inneggianti a imprese terroristiche[408].

Terzo criterio da valutare nel corso del giudizio di pericolosità cibernetica è la *modalità del soggetto di reagire alle pubblicazioni altrui*. In altri termini l'interprete dovrà valutare il *tenore* ed i *destinatari* dei *commenti* - che possono essere di disapprovazione (si pensi ad *hate speeches* verso minoranze religiose, etniche o politiche della popolazione dello Stato) o di approvazione (i quali potrebbero dunque rivelare l'adesione a idee o ad altre manifestazioni estremistiche) -, delle *condivisioni* di *pubblicazioni* altrui (magari effettuate su *social networks* diversi da quello in cui vengono riproposte) e delle *reactions*, che possono rivelare la posizione del soggetto rispetto a determinate idee, ancora una volta in senso di approvazione o disapprovazione.

A questi tre criteri, indicativi della speciale pericolosità cibernetica, l'interprete dovrà affiancare, in ogni caso, gli indici che, sulla base del d.lgs. 159/2011 e degli insegnamenti giurisprudenziali in materia, rilevano, in generale, ai fini della valutazione della pericolosità sociale *ex* art. 4, lett. d) del Codice

---

[408] Sul punto si veda il Considerando n. 11 della Direttiva (UE) 2017/541, in cui si prevede che il reato di auto-addestramento, posto in essere attraverso l'utilizzo della rete internet, postula, sotto il profilo oggettivo, una condotta attiva e, sotto quello soggettivo, l'intento di commettere o di contribuire a commettere un reato di terrorismo. Lo stesso Considerando, inoltre, fornisce alcuni *criteri* per valutare se una condotta compiuta nel *cyberspace* integri o meno il reato di auto-addestramento, i quali possono essere valorizzati nel giudizio volto a valutare la pericolosità del soggetto che abbia posto in essere atti preparatori obiettivamente rilevanti alla commissione del reato di cyberterrorismo: «Pertanto, scaricare un manuale al fine di fabbricare esplosivi per commettere un reato di terrorismo potrebbe essere assimilato all'atto di ricevere un addestramento a fini terroristici. Al contrario, il semplice fatto di visitare siti *web* o di raccogliere materiale per finalità legittime, ad esempio a scopi accademici o di ricerca, non è considerato ricezione di addestramento a fini terroristici ai sensi della presente direttiva».

antimafia. Il giudice sarà pertanto chiamato a valutare anche i comportamenti tenuti dal proposto fuori dal *cyberspace*, rilevando in proposito i rapporti intrattenuti dallo stesso con soggetti che abbiamo già commesso dei reati di terrorismo o *cyberterrorism*, la connivenza rispetto alla commissione degli stessi, i rapporti – purché non integranti un concorso esterno – con associazioni *ex* art. 270-*bis* c.p. o, ancora, la commissione di passati illeciti (non solo penali) peculiarmente di tipo cibernetico.

Così tassativizzati i criteri da impiegare nel giudizio di *pericolosità sociale cibernetica*, i critici potrebbero obiettare che essi costituiscono nulla più che dei meri indizi.

Sul punto si è già osservato che il giudizio per l'irrogazione delle misure di prevenzione – diversamente da quello penale – non si fonda su prove *strictu sensu*. Esso, infatti, non ha ad oggetto la dimostrazione della responsabilità per la commissione di un fatto di reato, bensì l'accertamento della circostanza che il soggetto proposto appartenga ad una delle categorie soggettive astrattamente previste dalla legge e della probabilità che egli commetta il reato (pericolosità sociale).

Sotto un diverso profilo, giova osservare che il paradigma indiziario consente di esaminare, con maggiore *flessibilità*, i segnali provenienti dal *cyberspace*, rispetto al quale, come si è detto, i rigidi canoni tradizionali del diritto penale (sostanziale e processuale) dimostrano notevoli difficoltà applicative. Invero i modelli della prova rappresentativa, testimoniale e documentale, in relazione a fatti accaduti nello spazio cibernetico, potrebbero rivelarsi scarsamente efficaci.

Ad ogni buon conto, fermo quanto sopra, anche nel giudizio di pericolosità cibernetica devono essere rispettate le garanzie previste per la materia penale, tra le quali, nella versione rafforzata elaborata dalla Corte Costituzionale nella sentenza 24/2019, figura la riserva di giurisdizione.

5.2. Le singole misure di prevenzione contro il cyberterrorismo: spunti dal diritto sovranazionale e nazionale

Tra gli obiettivi del presente lavoro figura l'individuazione, *de iure condendo*, di efficaci misure di prevenzione contro il cyberterrorismo, ferma la loro irrogazione sulla base di un previo giudizio di pericolosità, che deve essere soggetto alla riserva di giurisdizione ed alle altre garanzie previste in materia penale. Tale giudizio, per evitare arbitrarie compressioni della libertà personale in fase *ante delictum*, deve svolgersi in concreto ed avere ad oggetto la valutazione di criteri dotati di una base legale determinata e connotati da sufficiente tassatività, onde garantire ai consociati la prevedibilità delle conseguenze dei loro comportamenti.

Tanto premesso, rileva osservare che l'attuale strumentario italiano delle misure di prevenzione, sostanzialmente immutato dal 2011 (eccettuate le modifiche apportate al Codice Antimafia con l. 17.10.2017, n. 161) e affetto dai problemi di legittimità costituzionale precedentemente esaminati - che solo la giurisprudenza ha cercato di risolvere in via interpretativa -, è inadeguato a contrastare il fenomeno del terrorismo cibernetico[409].

Tale inadeguatezza emerge anche in relazione alla stessa *summa divisio* che connota le misure di prevenzione: personali o patrimoniali. *Tertium non datur*.

Ebbene, a tacere dei presupposti specifici di tipo soggettivo e oggettivo, che rispettivamente le due categorie postulano per la loro applicazione, è chiaro che le misure personali possono applicarsi solo ove sia individuato l'autore degli atti di cui alle lettere d) o h) dell'art. 4, d.lgs. 159/2011. Le misure patrimoniali,

---

[409] Cfr. F. BASILE, *Dieci anni di codice antimafia – le misure di prevenzione: bilanci e prospettive*, in *Rivista di Studi e Ricerche sulla criminalità organizzata*, 3/2021, pp. 16-19, in cui l'autore, dopo aver evidenziato che il sistema delle misure di prevenzione disciplinato nel d.lgs. 159/2011 è rimasto sostanzialmente immutato nell'arco di dieci anni, rappresenta soltanto un punto di partenza per un intervento sistematico del legislatore che - diversamente da quanto parte della dottrina sostiene - deve riconoscere il carattere fortemente afflittivo delle misure di prevenzione e assoggettarle a garanzie analoghe a quelle della materia penale.

invece, possono trovare applicazione anche a prescindere dai presupposti soggettivi - tanto che, come si è evidenziato, l'art. 18 d.lgs. 159/2011 ne consente l'irrogazione anche in caso di carenza di attualità della pericolosità sociale o, addirittura, in caso di morte del soggetto che ha posto in essere gli atti rilevanti a norma della disposizione da ultimo richiamata - postulando, in ultima analisi, l'esistenza di beni rispetto ai quali applicare direttamente le misure[410].

Conseguentemente è evidente che le *misure di prevenzione tradizionali* potranno essere irrogate, rispetto al terrorismo cibernetico, esclusivamente nel caso in cui sia possibile individuare l'autore degli atti posti in essere *online* (eventualmente limitandone la libertà personale) o i beni che costituisco il prezzo, il prodotto, il profitto degli atti compiuti o, ancora, i mezzi per realizzarli (disponendone il sequestro o la confisca).

Tuttavia l'impostazione che richiede, per il cyberterrorismo, la necessaria individuazione del soggetto agente o dei beni per l'applicazione delle misure di prevenzione appare alquanto miope, dal momento che, da un lato, è ancorata alla struttura dei reati informatici e, dall'altro lato, ignora che il cyberspazio è, per sua stessa natura, depersonalizzato e dematerializzato, con incompatibilità rispetto ai canoni soggettivi ed oggettivi classici.

Si ritiene dunque necessario elaborare delle misure che possano applicarsi *ante delictum* anche a prescindere dall'individuazione del proposto o dei suoi beni, la quale nel *cyberspace* nella maggior parte dei casi non è agevole.

Tali nuove misure, sulla base delle considerazioni ampiamente svolte nei Capitoli I e II del presente lavoro, saranno astrattamente riconducibili entro l'alveo delle misure personali e non, invece, di quelle patrimoniali. Detta impostazione può essere condivisa se si accoglie l'idea che l'utilizzo di *Internet* e più in generale dei sistemi e delle reti informative - con l'immissione di *dati* ed *informazioni che riguardano la persona* - non possono intendersi quali beni patrimoniali (art. 635-*bis* c.p.) o, peggio, quali estensioni del domicilio (art. 615-*ter* c.p.). Diversamente essi sono *proiezioni virtuali della persona umana*, la

[410] In proposito si veda il precedente §. 4.1. di questo Capitolo.

quale, nello spazio cibernetico, deve essere intesa alla stregua di un fascio di dati e informazioni, tale da esprimere la propria personalità ed esercitare la propria libertà, che vanno tutelate[411].

Fermo quanto sopra, è evidente che, per individuare le nuove misure di prevenzione contro il terrorismo cibernetico, sia preliminarmente necessario guardare - in un'ottica comparatistica - al sistema di fonti multisettoriali del diritto europeo in materia, già esaminate nel precedente Capitolo. Infatti, come si è evidenziato, il diritto eurounitario ha impostato la strategia per il contrasto del *cybercrime* e del terrorismo *online* in un'ottica di prevenzione, indicando, in atti di diritto derivato, nuove misure.

In sede di applicazione delle stesse, si ritiene necessario valorizzare le potenzialità delle tecnologie cibernetiche, onde consentire allo Stato di contrastare, con adeguata efficacia, l'impiego abusivo abilmente fattone da parte dei terroristi[412].

In ambito militare si impiega da decenni la tecnologia cibernetica per contrastare gli attacchi ai sistemi di difesa e, pertanto, appare utile valutare se questo settore offra degli spunti per prevenire efficacemente gli atti di quei

---

[411] Sul concetto di *habeas data* S. RODOTÀ, *Discorso del Presidente Stefano Rodotà*, nella *Relazione annuale del Garante della Privacy*, op. cit., p. 16. *Dati* ed *informazioni* sono strumenti attraverso i quali si manifesta la libertà e la personalità degli individui, tanto che l'autore ravvisa la necessità di tutelare adeguatamente ed in via autonoma il loro «*corpo elettronico*», invocando un «*habeas data*», quale indispensabile sviluppo dell'*habeas corpus*.

[412] È auspicabile che il legislatore italiano valorizzi gli strumenti tecnologici, impiegandoli sistematicamente per elaborare nuove misure di prevenzione per il contrasto del cyberterrorismo, la cui maggiore pervasività è legata all'abile utilizzo che i terroristi hanno saputo fare delle tecnologie cibernetiche. La più autorevole dottrina in materia si è espressa criticamente rispetto alla sfiducia, dimostrata dal legislatore, con riguardo all'impiego delle tecnologie per il contrasto del reato in parola. In tal senso si è espresso R. FLOR, *Cyber-terrorismo e diritto penale in Italia*, in AA.VV., R. WENIN, G. FORNASARI (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo*, *sviluppo tecnologico e garanzie fondamentali*, ed. Università degli Studi di Trento, 2017, p. 357, cui si legge che: «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»; A. F. VIGNERI, *Cyberterrorismo: realtà o finzione? profili problematici di definizione e contrasto*, op. cit., pp. 8 e ss.

soggetti che, pur in tempo di pace, agiscono con la stessa violenza del nemico e, se possibile, con spietatezza maggiore[413].

Ad ogni buon conto giova osservare che il legislatore italiano, in alcuni settori, ha riconosciuto la minaccia cibernetica ed è intervenuto per *prevenirla* con la legislazione speciale, peculiarmente nelle materie della *responsabilità delle persone giuridiche* (d.lgs. 231/2001) e del *cyberbullismo* (l. 71/2017), alle quali sarà opportuno guardare per elaborare un'efficace risposta anche in ambito cyberterroristico.

5.2.1. Le misure di prevenzione di matrice eurounitaria contro il cyberterrorismo

Nel precedente Capitolo di questo lavoro si sono esaminate partitamente le fonti del diritto europeo - anche non penali - che rilevano in materia di cyberterrorismo. Nel presente paragrafo si intende proporne una sintesi critica, evidenziando quali, tra le misure elaborate dal legislatore sovranazionale, appaiano compatibili, *lato sensu*, rispetto ai principi del diritto penale costituzionalmente orientato - che la giurisprudenza della Consulta ritiene vadano applicati alle misure di prevenzione -, potendo così essere impiegate con funzione preventiva del cyberterrorismo.

Ebbene, per prevenire i *cybercrimes* e quindi il cyberterrorismo, l'Europa sostiene convintamente la necessità che gli Stati membri, le loro Autorità Giudiziarie e le Istituzioni eurounitarie cooperino per lo scambio di informazioni. L'assidua *cooperazione* è l'unico strumento capace di assicurare il costante

---

[413] Sul tema F. VIGANÒ, *Terrorismo, guerra e diritto penale*, in *Riv. It. dir. proc. pen*., 4/2006, pp. 694 e ss.; M. TRAPANI, *Guerra e diritto penale. Sull'adeguatezza degli strumenti penalistici nei confronti del c.d. terrorismo islamico*, in AA.VV., *Politica criminale e cultura giuspenalistica*. *Scritti in onore di Sergio Moccia*, Jovene, 2017, pp. 253 e ss.; sul rischio di confondere la legislazione penale dell'emergenza per il contrasto del terrorismo con il diritto di guerra, invece, R. BARTOLI, *Lotta al terrorismo internazionale. Tra diritto penale del nemico, jus in bello criminale e annientamento del nemico assoluto*, Giappichelli, 2008, pp. 177 e ss.

controllo delle reti, dei sistemi informativi e, in ultima analisi, del *cyberspace*, che, come si è spiegato, non può essere ristretto entro i confini nazionali.

In proposito appare particolarmente utile la creazione di un «*punto di contatto*» (art. 8 della direttiva 2016/1148/UE) specificamente dedicato al cyberterrorismo, che garantirebbe, anche in questa materia, un'attiva cooperazione transfrontaliera tra le Autorità competenti dei diversi Stati membri.

L'Unione europea, inoltre, ha istituito numerose Agenzie e strutture per la *cybersecurity*, le quali, tra i loro principali obiettivi, annoverano proprio il raggiungimento di un livello comune di sicurezza contro il crimine cibernetico tra i diversi Paesi membri, nonché la promozione di un'intensa cooperazione fra gli stessi, per prevenire il fenomeno.

Tra queste, l'Agenzia europea per la cybersicurezza (ENISA) promuove, sin dalla sua istituzione, la cooperazione fra gli Stati membri per lo scambio di informazioni e per la prevenzione del crimine cibernetico. Tale peculiare funzione andrebbe rafforzata e svolta in stretta collaborazione con l'*European Cybercrime Centre* (EC3)[414].

Nella medesima ottica di cooperazione operano i «*gruppi di intervento per la sicurezza informatica in caso di incedente*» (CSIRT), *ex* art. 9 della direttiva 2016/1148/UE. Questi, come si è visto, hanno il compito di monitorare, intercettare e analizzare le minacce cibernetiche rivolte agli enti pubblici e privati. I *gruppi* - interpretando la *ratio* preventiva che anima la strategia europea contro il cyberterrorismo – si occupano di elaborare un protocollo per stabilire se e come un attacco e, prima ancora, una minaccia possano impattare su un determinato ente, quali siano i metodi più adatti per contenerli e neutralizzarli, quale soggetto debba occuparsi di informare e aggiornare gli *stakeholders* sullo stato delle minacce e sulle azioni di risposta.

L'istituzione di un gruppo di intervento presso ogni infrastruttura critica dello Stato consentirebbe la predisposizione di protocolli *ad hoc*, con il costante

---

[414] L'*European Cybercrime Centre* (EC3) è il corpo di *Europol* che coordina le attività transfrontaliere delle forze dell'ordine contro il crimine cibernetico (*https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3*).

monitoraggio delle minacce cibernetiche e la possibilità di prevenire tempestivamente la commissione dei reati cyberterroristici. I gruppi di intervento in parola dovrebbero essere composti da esperti di cibernetica e di terrorismo, che collaborando interpretino correttamente il significato degli atti compiuti nel *cyberspace*.

Ad ogni buon conto il diritto eurounitario, più concretamente, individua specifiche *misure negative* che possono impiegarsi per prevenire il cyberterrorismo, intervenendo rispetto agli atti ed ai comportamenti che - rilevando a norma dell'art. 4, lettere d) e h) del d.lgs. 159/2011 – sono sintomatici della pericolosità sociale cibernetica.

Trattasi delle misure della *rimozione*, del *blocco* e della *disabilitazione* dei contenuti terroristici *online*, le quali, così come previste dagli artt. 21 della direttiva (UE) 2017/541 e 3 del regolamento 2021/784, riguardano contenuti la cui pubblicazione integra già di per sé reato, risultando così legate da un rapporto ancillare rispetto alla pena. Ciononostante, pare potersi ritenere che tali misure, in ragione della loro natura, possano essere utilmente applicate anche in fase *ante delictum*, con la funzione di prevenire la commissione del reato. Esse, infatti, permetterebbero di rimuovere radicalmente pubblicazioni dotate di *obiettiva rilevanza* rispetto alla commissione di condotte cyberterroristiche, ad esempio *posts* capaci di condizionare le scelte politiche degli utenti o *links* che - secondo il modello del *trojan horse* - una volta aperti possono infettare il sistema informatico preso di mira, causandone il malfunzionamento.

In particolare, la misura del *blocco dell'accesso ai contenuti* - la quale, a norma dell'art. 21, par. 2, direttiva 2017/541, può essere applicata solo ove non sia possibile procedere alla rimozione - potrebbe essere utilizzata in via principale rispetto ad *account*, pagine o, più in generale, siti che pubblicano materiale idoneo a condizionare la libertà di scelta politica di coloro che vi accedono. Si tratterebbe di una misura meno limitante rispetto alla rimozione, dal momento che i contenuti non verrebbero radicalmente eliminati e che l'impedimento alla loro consultazione potrebbe essere solo temporaneo, magari per la durata della campagna elettorale in corso di svolgimento.

Parimenti, il regolamento (UE) 2021/784 prevede specifiche misure per il contrasto della diffusione dei contenuti terroristici *online*, che potrebbero essere impiegate in fase predelittuale.

Trattasi in particolare degli *ordini di rimozione* e di *disabilitazione* previsti dall'art. 3 del suddetto regolamento.

La disposizione offre interessanti spunti di riflessione sotto il profilo procedurale. In primo luogo, giova rilevare che - soddisfacendo il principio della riserva di giurisdizione sancito dalla Consulta nella sentenza 24/2019 - l'Autorità competente, legittimata ad ordinare la rimozione o la disabilitazione, può essere esclusivamente quella Giudiziaria (art. 3, par. 1). L'applicazione della misura presuppone l'accertamento (in un apposito giudizio di pericolosità) della probabilità che il proposto - se individuabile - commetta un reato di cyberterrorismo e, in ogni caso, dell'obiettiva rilevanza dei contenuti pubblicati rispetto alla commissione del reato[415].

L'ordine di rimozione, corredato di dettagliate istruzioni sulle procedure da seguire[416], deve essere indirizzato al prestatore di servizi di *hosting*[417], il quale

---

[415] Sul punto rileva osservare che l'art. 3, par. 2 del regolamento (UE) 2021/784 precisa che l'ordine di rimozione può essere applicato solo qualora sussistano «*casi di emergenza debitamente giustificati*». Orbene, pare potersi ritenere che l'intervento, in funzione preventiva, per impedire la commissione di un atto di cyberterrorismo sia tale da giustificare l'emanazione della misura in esame.

[416] A norma dell'art. 3, par. 4, del regolamento in esame, gli ordini di rimozione devono contenere i seguenti elementi: a) dati identificativi dell'autorità competente che emette l'ordine di rimozione e l'autenticazione dell'ordine di rimozione da parte di tale autorità competente; b) la motivazione, sufficientemente dettagliata, per cui i contenuti sono considerati contenuti terroristici e un riferimento alle pertinenti tipologie di materiale di cui all'art. 2, punto 7; c) un indirizzo URL (*Uniform Resource Locator*) esatto e, se necessario, ulteriori informazioni che consentano di individuare i contenuti terroristici; d) un riferimento al presente regolamento come base giuridica dell'ordine di rimozione; e) la data, l'ora e la firma elettronica dell'autorità competente che emette l'ordine di rimozione; f) informazioni facilmente comprensibili sui mezzi di ricorso a disposizione del prestatore di servizi di *hosting* e del fornitore di contenuti, ivi comprese informazioni sul ricorso all'autorità competente, il ricorso a un organo giurisdizionale nonché sui termini per il ricorso; g) ove necessario e proporzionato, la decisione di non divulgare informazioni sulla rimozione o sulla disabilitazione dell'accesso ai contenuti terroristici conformemente all'art. 11, par. 3.

[417] L'art. 3, par. 5 del regolamento in esame prevede che l'autorità competente indirizzi l'ordine di rimozione allo stabilimento principale del prestatore di servizi di *hosting* o al suo

è tenuto a darvi esecuzione entro il breve termine di un'ora dalla ricezione dello stesso[418].

5.2.2. Spunti di riflessione per le misure di prevenzione contro il cyberterrorismo dal settore militare e dell'Intelligence

La prevenzione ed il contrasto degli attacchi cibernetici figurano tra i principali obiettivi dell'amministrazione militare degli Stati, che essa persegue impiegando tecnologie avanzate e strategie sofisticate. Queste ultime possono rappresentare degli strumenti per prevenire efficacemente, ancorché in tempo di pace, la commissione di reati con finalità di terrorismo e, specificamente, di cyberterrorismo, i quali sono connotati da un tasso di violenza (anche solo morale) e di spietatezza almeno pari a quello che si registra in guerra[419].

La strategia militare per prevenire gli attacchi cibernetici poggia sui pilastri della *cooperazione a livello internazionale* e della predisposizione di *protocolli per intercettare tempestivamente il rischio di attacchi*, secondo un approccio che, per certi versi, ricalca quello adottato dall'Unione europea in materia.

---

rappresentante legale. Questo, a norma dell'art. 17 dello stesso regolamento, deve essere designato per iscritto e deve risiedere o essere stabilito in uno degli Stati membri in cui il prestatore di servizi di *hosting* offre i propri servizi.

[418] L'art. 3, par. 7 del regolamento contempla il caso in cui il prestatore di servizi di *hosting* non sia in grado di conformarsi all'ordine di rimozione per cause di forza maggiore o di impossibilità di fatto a lui non imputabile (compresi i motivi tecnici od operativi obiettivamente giustificabili). In un caso siffatto il prestatore di servizi di *hosting* ne informa, senza indebito ritardo, l'Autorità competente che ha emesso l'ordine di rimozione spiegando i motivi. Il termine di un'ora decorrerà dal momento in cui i motivi, che hanno impedito di eseguire l'ordine, vengono meno.

[419] Sul punto basti pensare che nel 2020 il Ministero della Difesa ha istituito il *Comando per le Operazioni in Rete* (COR), nel quale è confluito il *Comando Interforze per le Operazioni Cibernetiche* (CIOC), la cui funzione principale consiste nel contrastare gli attacchi cibernetici alle infrastrutture critiche nazionali, settore nel quale collabora con *l'Agenzia Nazionale della Cybersecurity* (ANC).

Con riguardo al primo pilastro, si segnala che nel 2008 è stato istituito, presso la NATO, il *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), con sede a Tallinn. Trattasi di un'organizzazione militare volta a migliorare la cooperazione e la condivisione di informazioni per la difesa cibernetica tra i Paesi NATO, attraverso iniziative di formazione, ricerca e sviluppo. In particolare il Centro si propone di fornire competenze in materia di cybersicurezza alle Autorità dei Paesi membri della NATO coinvolte nel settore e di contribuire all'evoluzione del diritto internazionale in materia[420].

Nella stessa ottica di cooperazione, l'ONU, che tra le sue funzioni annovera il mantenimento della pace e della sicurezza mondiale, ha promosso l'istituzione dell'*International Multilateral partnership against cyber-terrorism* (IMPACT), con sede a Kuala Lumpur (Malesia), per la collaborazione a livello internazionale in materia di prevenzione e contrasto del cyberterrorismo[421]. L'IMPACT è un partenariato che coinvolge gli Stati membri dell'ONU, enti pubblici, soggetti privati (in particolare attori economici impegnati nei settori della difesa e delle tecnologie informatiche), professionisti ed accademici esperti in materia di *cybercrimes* e terrorismo. Tali soggetti collaborano nello svolgimento di attività di ricerca, studio e catalogazione delle minacce cyberterroristiche, nonché nell'elaborazione di misure di prevenzione del fenomeno[422].

Per quanto attiene al secondo pilastro, consistente nella predisposizione di *protocolli per intercettare tempestivamente il rischio di attacchi*, si segnala che,

---

[420] Per una panoramica degli obiettivi perseguiti dal *Cooperative Cyber Defence Centre of Excellence*, si rinvia al sito istituzionale: *https://ccdcoe.org/*. L'organismo, come si è detto nel primo Capitolo del presente lavoro, ha promosso il gruppo di studio che ha redatto i cosiddetti Manuali di Tallinn.

[421] Oggi l'organismo in parola ha cambiato denominazione in *International Multilateral partnership against cyber-threats*, al fine di ricomprendere tutti i possibili attacchi cibernetici.

[422] L'istituto in parola è il braccio operativo dell'*International Telecomunication Union* (ITU), ovverosia l'Agenzia dell'ONU che si occupa di favorire lo sviluppo e l'efficace sfruttamento dei mezzi di telecomunicazione. Altre organizzazioni internazionali che hanno promosso la cooperazione tra gli Stati in materia di contrasto ai *cybercrimes* sono l'*Associazione delle Nazioni del Sudest Asiatico* (ASEAN), l'*Organizzazione degli Stati Americani* (OSA) e la *Shanghai Cooperation Organization* (SCO).

con direttiva SMD-I-013 intitolata "*Procedure di risposta agli incidenti informatici riguardanti le reti telematiche della Difesa*" (ed. 2017), lo Stato Maggiore della Difesa italiano ha elaborato una dettagliata procedura per prevenire gli incidenti informatici, minimizzarne l'eventuale impatto sulle infrastrutture critiche dello Stato e supportare le successive attività di ripristino. Il protocollo in parola si articola in tre fasi, secondo la dinamica del *cyberattack*: *pre-attacco*, *attacco* e *post-attacco*[423].

La direttiva prevede che nel corso della fase di *pre-attacco* vengano attuate delle *Procedure Operative Standard* (POS) per monitorare tutte le risorse (umane, materiali ed immateriali-informative) di una determinata infrastruttura critica. Dette procedure devono prevedere: la classificazione del sistema informativo tutelando e le sue caratteristiche; la classificazione degli incidenti che possono interessarlo e dei conseguenti interventi; l'elenco completo del personale tecnico qualificato preposto alla gestione dell'incidente; le procedure di coordinamento con organi esterni preposti alla sicurezza[424].

Inoltre, la fase di pre-attacco prevede l'impiego di appositi *software* detti *Intrusion Prevention Systems* (IPS), che, attraverso algoritmi, confrontano i flussi di dati, che penetrano nel sistema informatico dall'esterno, con le informazioni contenute in un *database*, ove è presente un elenco dei *malwares* e delle forme di attacchi cibernetici già noti. Il confronto operato dall'*IPS* consente di stabilire se vi sia coincidenza fra i dati in ingresso e i modelli registrati, segnalando, in caso affermativo, la possibilità che si verifichi un attacco e, quindi, l'opportunità di applicare delle misure di prevenzione[425].

---

[423] Per un esame dettagliato, anche sotto il profilo tecnico, della *timeline* del *cyberattack* F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018, pp. 249 e ss.; S. LISI, U. GORI, *Information warfare 2012. Armi cibernetiche e processo decisionale*, Franco Angeli, 2013, p. 83.

[424] Per una panoramica sulle *Procedure Operative Standard*, si veda la Direttiva dello Stato Maggiore della difesa "*Sicurezza dei Sistemi Informatici e di Telecomunicazione non classificati*" (SME INFOSEC 001) del 29.9.2010.

[425] Sul tema degli *Intrusion Prevention Systems* si veda B. GUPTA, S. SRINIVASAGOPALAN, *Handbook of Research on Intrusion Detection Systems*, IGI Global, 2020, pp. 77 e ss.

La prevenzione ed il contrasto delle minacce cibernetiche ed in particolare cyberterroristiche figurano tra gli obiettivi principali anche dei servizi di *intelligence* nazionali.

Per quanto riguarda l'Italia, il *Sistema di informazione per la sicurezza della Repubblica* (SISR), negli anni 2020 e 2021, ha intensificato il suo impegno nel *cyberspace*, al fine di garantire la tutela delle infrastrutture nazionali, attesa la sensibile crescita di azioni *cyber* di matrice criminale, registratasi proprio in coincidenza della pandemia da COVID-19[426]. Come emerge dai risultati dell'attività di monitoraggio condotta dal *Dipartimento delle informazioni per la sicurezza* (*DIS*), le attività *cyber* ostili - tra cui quelle con finalità cyberterroristica - hanno interessato prevalentemente enti pubblici e, più in generale, «*assetti informatici rilevanti per la sicurezza nazionale*». Tali attività si sono rivolte alle infrastrutture informatiche della Pubblica Amministrazione (69%), delle Amministrazioni centrali dello Stato (56%) ed a quelle degli enti locali e delle strutture sanitarie (30%)[427].

Al fine di fronteggiare il crescente numero di *cybercrimes*, con il d.l. 14.6.2021, n. 82 (convertito in l. 4.8.2021, n. 109), si è provveduto alla radicale riorganizzazione dell'architettura *cyber* nazionale. Sono state così attribuite nuove competenze esclusive al Presidente del Consiglio dei Ministri, tra le quali l'alta direzione e la responsabilità generale delle politiche in materia di *cybercrimes*, e sono stati istituiti il *Comitato interministeriale per la cybersicurezza* (con funzioni di consulenza, proposta e vigilanza) e l'Agenzia per la Cybersicurezza Nazionale (ACN). Quest'ultima si propone di potenziare la cyberresilienza del Paese,

---

[426] Secondo quanto si legge nella *Relazione annuale 2021 del Sistema di informazione per la sicurezza della Repubblica*, p. 20, al link: *https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2022/02/RELAZIONE-ANNUALE-2021.pdf*, il modello di *cyberattack* prevalente è il *Ransomware-as-a-Service* (RaaS). Esso si basa sull'interazione tra due soggetti: «da un lato, gli sviluppatori dell'arma digitale e, dall'altro, parti terze che, dopo aver condotto attacchi nei confronti dei target d'interesse, cedono ai primi una parte degli introiti illeciti eventualmente ottenuti».

[427] Sul punto di veda la *Relazione annuale 2021 del Sistema di informazione per la sicurezza della Repubblica*, cit., p. 40, in particolare la Tabella IV.

riducendone il grado di vulnerabilità e incrementandone l'autonomia e l'indipendenza tecnologica[428].

5.2.3. Le misure di prevenzione dei reati cibernetici nella legislazione speciale: il modello di organizzazione, gestione e controllo previsto dal d.lgs. 231/2001 sulla responsabilità da reato delle persone giuridiche

Il legislatore italiano, fermo il sistema codicistico delle fattispecie delittuose per il contrasto dei reati informatici, si occupa delle misure di prevenzione dei *cybercrimes* in almeno due leggi speciali.

La prima è la normativa dedicata alla disciplina della responsabilità delle persone giuridiche, delle società e delle associazioni (anche prive di personalità giuridica), prevista dal d.lgs. 8.6.2001, n. 231, sulla natura della quale, come noto, tuttora si dibatte[429].

Essa prevede che gli enti giuridici possano essere ritenuti responsabili nel caso in cui persone fisiche ad essi appartenenti commettano - al ricorrere di

---

[428] *Relazione annuale 2021 del Sistema di informazione per la sicurezza della Repubblica*, cit., p. 12, in particolare il Box 1. L'*Agenzia per la Cybersicurezza Nazionale* si propone di tutelare gli interessi nazionali nel campo della *cybersecurity* e provvede, tra l'altro, a coordinare i soggetti pubblici coinvolti nel settore a livello nazionale, promuovendo: la realizzazione di azioni comuni dirette a garantire la sicurezza e resilienza cibernetiche; la predisposizione della strategia nazionale di cybersicurezza; l'assunzione di tutte le funzioni della Presidenza del Consiglio dei Ministri in materia di perimetro di sicurezza nazionale cibernetica, nonché quelle già attribuite al DIS; lo sviluppo delle capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e i relativi attacchi (anche attraverso il CSIRT Italia). Inoltre, l'*Agenzia per la Cybersicurezza Nazionale* agisce in qualità di *punto di contatto unico* in materia di sicurezza delle reti e dei sistemi informativi, nonché di *Autorità nazionale di certificazione della cybersicurezza*. Presso l'Agenzia è stato costituito, in via permanente, il *Nucleo per la cybersicurezza*, che supporta il Capo del Governo per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

[429] Sulla controversa natura giuridica della responsabilità degli enti collettivi prevista dal d.lgs. 231/2001 R. GAROFOLI, *Il contrasto ai reati di impresa nel d.lgs. n. 231 del 2001 e nel d.l. n. 90 del 2014: non solo repressione, ma prevenzione e continuità aziendale*, in *Dir. Pen. Cont*., 30.9.2015, pp. 2 e ss.; G. DE SIMONE, *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione*, *Dir. Pen. Cont*., 2012, pp. 5 e ss.

specifiche condizioni soggettive e oggettive[430] - uno dei reati tassativizzati agli artt. 24 e ss. del d.lgs. 231/2001. Tra questi figurano i *delitti informatici* (art. 24-*bis*)[431] e tutti i *reati con finalità di terrorismo e di eversione dell'ordine democratico* (art. 25-*quater*).

Gli artt. 6 e 7 del d.lgs. 231/2001, inoltre, prevedono che gli enti in questione sono tenuti ad adottare ed attuare efficacemente un *modello organizzativo*, *di gestione e controllo*, il quale possiede una duplice funzione.

Sotto un primo profilo, il *modello* deve essere idoneo a prevenire i reati-presupposto, attraverso la previsione di misure atte a garantire lo svolgimento dell'attività dell'ente e a scoprire ed eliminare tempestivamente situazioni di rischio, in relazione alla natura ed alla dimensione dell'organizzazione, nonché al tipo di attività svolta.

---

[430] R. GAROFOLI, *Il contrasto ai reati di impresa nel d.lgs. n. 231 del 2001 e nel d.l. n. 90 del 2014: non solo repressione, ma prevenzione e continuità aziendale*, op. cit., pp. 4. La disciplina dettata dal d.lgs. 231/2001 trova applicazione nei confronti di enti forniti di personalità giuridica e di società o associazioni, anche prive di personalità giuridica. Diversamente, essa non opera rispetto allo Stato, agli enti pubblici territoriali, e agli altri enti pubblici non economici (art. 1, co. 3). La responsabilità degli enti presuppone la commissione di uno dei cosiddetti reati presupposto, tassativizzati dall'art. 24 del d.lgs. 231/2004. Detto reato deve essere commesso per favorire l'ente e, quindi, per il perseguimento di un suo interesse o vantaggio (art. 5). Inoltre, sotto il profilo dei soggetti, il reato deve essere commesso da un soggetto che occupa una posizione apicale (legato all'ente da un rapporto di rappresentanza, amministrazione, gestione o controllo), da persone che esercitano, anche di fatto, la gestione e il controllo dell'ente (art. 5, lett. a) oppure da soggetti sottoposti alla vigilanza o direzione dei primi (art. 5, lett. b).

[431] I reati presupposto di tipo informatico previsti dall'art. 24-*bis* del d.lgs. 231/2001 sono: l'"*Accesso abusivo a un sistema informatico o telematico*" (art. 615-*ter* c.p.); la "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*" (art. 615-*quater* c.p.); la "*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*" (art. 615-*quinquies* c.p.); l'"*Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche*" (art. 617-*quinquies* c.p.); l'"*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*" (art. 617-*quater* c.p.); il "*Danneggiamento di informazioni, dati e programmi informatici*" (art. 635-*bis* c.p.); il "*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*" (art. 635-*ter* c.p.); il "*Danneggiamento di sistemi informatici o telematici*" (art. 635-*quater* c.p.); il "*Danneggiamento di sistemi informatici o telematici di pubblica utilità*"(art. 635-*quinquies* c.p.); la "*Frode informatica del certificatore di firma elettronica*" (art. 640-*quinquies* c.p.).

Sotto un secondo profilo, poi, l'adozione e l'efficace attuazione del *modello* rileva – unitamente ad altre condizioni - quale esimente da responsabilità dell'ente[432].

Orbene, il modello di gestione, organizzazione e controllo previsto dagli artt. 6 e 7 del d.lgs. 231/2001 soddisfa la *ratio* preventiva che ha animato il legislatore europeo nell'elaborazione della strategia per il contrasto del terrorismo *online*. Esso, infatti, si colloca a pieno titolo tra le misure di prevenzione positiva e specificamente tra le *best practices*, ricomprendendo, fra i reati presupposto, anche il terrorismo.

Tuttavia il modello, al fine di ricevere concreta applicazione anche per la prevenzione dei reati di cyberterrorismo che potrebbero essere commessi dall'ente, richiede alcuni interventi adeguatori.

In primo luogo, è necessario che il legislatore aggiorni l'elenco tassativo dei reati presupposto – che già prevede i reati informatici - aggiungendo i *cybercrimes*, i quali, come si è detto, restano attualmente ignoti al nostro ordinamento.

In secondo luogo, sarebbe opportuno consentire l'adozione del modello di organizzazione, gestione e controllo anche da parte degli enti pubblici (peculiarmente delle infrastrutture critiche dello Stato), ai quali la disciplina dettata dal d.lgs. 231/2001 resta preclusa in forza dell'espressa previsione del relativo art. 1, co. 3.

Infine, sotto un profilo eminentemente pratico, sarebbe necessario indicare gli specifici elementi che devono connotare il modello per l'efficace prevenzione dei reati con finalità di cyberterrorismo.

---

[432] Per un esame della funzione del modello di organizzazione, gestione e controllo previsto dal d.lgs. 231/2001, R. GAROFOLI, *Il contrasto ai reati di impresa nel d.lgs. n. 231 del 2001 e nel d.l. n. 90 del 2014: non solo repressione, ma prevenzione e continuità* aziendale, op. cit., pp. 3 e ss., in cui l'autore afferma che: «Di fronte alla crisi del modello punitivo-repressivo tradizionale, la strada intrapresa nell'ambito del diritto penale dell'economia è quella di una nuova politica di prevenzione. L'avvio di questa prospettiva risale all'inizio del nuovo millennio con il d.lgs. n. 231 del 2001 e la prevista responsabilità degli enti. Il modello prescelto è stato quello della responsabilità per l'omessa adozione delle cautele organizzative idonee ad impedire la commissione di reati da parte dei dipendenti o degli amministratori».

Sul punto rileva osservare che gli artt. 6, co. 1, lett. a) e 7, co. 2, d.lgs. 231/2001 postulano, come già evidenziato, che il modello sia connotato dall'*idoneità* a prevenire i reati presupposto tipizzati nello stesso decreto legislativo. Tale *idoneità* presuppone l'adozione di misure atte a garantire all'ente lo svolgimento della sua attività nel rispetto della legge ed a scoprire ed eliminare tempestivamente situazioni di rischio.

Ebbene, con riferimento alle infrastrutture critiche dello Stato, sarebbe necessario elaborare un modello connotato da maggiore complessità rispetto a quello impiegato dagli enti privati, tale da assicurare un'adeguata sorveglianza rispetto agli atti obiettivamente rilevanti diretti alla commissione dei reati cyberterroristici[433].

La concreta *idoneità* del modello dovrà quindi essere commisurata alla *natura pubblica* dell'infrastruttura tutelata e alla sua *dimensione nazionale*, nonché alle criticità connesse alle *attività* svolte dalla stessa nella "porzione" di *cyberspace* di sua competenza usato dai cittadini per comunicare[434].

---

[433] L'*Organizzazione internazionale per la normazione* (ISO) ha dettato dei criteri minimi che devono connotare il modello di organizzazione, gestione e controllo che le persone giuridiche sono tenute ad adottare. Detti criteri possono essere valorizzati, nell'ottica dell'armonizzazione internazionale in materia, rispetto alla creazione del modello di prevenzione contro il cyberterrorismo. In particolare, l'*Annex A* della norma ISO 27001 e le linee guida di implementazione di cui alla norma ISO 27002 - dedicate alla sicurezza informatica - prevedono che l'ente sia tenuto a dotarsi di alcuni protocolli minimi. Tra questi figurano: a) *Gestione degli assets*: l'infrastruttura critica deve identificare gli *assets* (*rectius* i beni giuridici) connessi alle informazioni di cui si occupa, documentando il loro trattamento; b) *Formazione del personale*: l'infrastruttura critica deve dotarsi di personale qualificato in materia di *cybercrimes* e reati terroristici, sottoponendolo a periodici corsi di aggiornamento, affinché disponga delle competenze per vigilare sull'efficace attuazione del modello; c) *Controllo degli accessi*: l'infrastruttura critica deve stabilire una politica di controllo degli accessi alle informazioni. Trattasi in particolare di limitare il più possibile il numero dei soggetti abilitati ad accedere alle informazioni rilevanti, prevedere requisiti stringenti per l'accesso e rivedere periodicamente i diritti d'accesso; d) *Sicurezza fisica e ambientale*: l'infrastruttura critica deve proteggere i luoghi (fisici e virtuali) che contengono informazioni sensibili o critiche, nonché le strutture di elaborazione delle informazioni; e) *Controlli operativi*: l'infrastruttura critica deve stabilire una serie di controlli operativi delle informazioni. Tra le misure più significative si annoverano i *backup* frequenti, le procedure interne per la gestione di errori o incidenti e i sistemi di protezione dai *malwares*.

[434] L'art. 7, co. 3, d.lgs. 231/2001 precisa che l'*idoneità* del modello organizzativo di gestione e controllo deve essere *valutata concretamente*, in relazione ai parametri della *natura* dell'ente, della *dimensione* della sua *organizzazione* e del *tipo di attività* che lo stesso svolge.

L'efficace attuazione, da parte delle infrastrutture critiche dello Stato, di un modello dotato di siffatti requisiti rappresenta un utile strumento, riconducibile all'alveo delle *best practices* (altamente qualificate sotto il profilo giuridico e tecnico), per impedire, sul nascere, il compimento di atti preparatori obiettivamente rilevanti diretti alla commissione di reati cyberterroristici da parte dell'ente[435]. Tale intervento, che idealmente potrebbe collocarsi in una fase addirittura anteriore a quella dell'applicazione delle misure negative (e quindi *pre-preventiva,* si potrebbe dire), risponde alla richiesta di intensificare la *positive prevention* avanzata dalle Istituzioni europee con le direttive 2016/1148 e 2017/541.

5.2.4. Le misure di prevenzione dei reati cibernetici nella legislazione speciale: la legge 71/2017 sulla prevenzione ed il contrasto del fenomeno del cyberbullismo

La seconda normativa speciale in cui il legislatore italiano si occupa di prevenzione dei *cybercrimes* è la legge 29.5.2017, n. 71, la quale è dedicata alla tutela dei minori per la prevenzione ed il contrasto del cyberbullismo.

La materia è interessata da talune delle criticità che sono emerse in relazione al cyberterrorismo. Infatti il bullismo cibernetico, la cui prevenzione è disciplinata *extra codicem*, è considerato un fatto penalmente rilevante, come emerge dalla definizione di cui all'art. 1, co. 2, l. 71/2017, ancorché ne manchi la tipizzazione in un'apposita fattispecie autonoma.

Con riguardo alle forme di manifestazione, a norma della succitata disposizione, il cyberbullismo può atteggiarsi alternativamente come «*pressione,*

---

[435] L. PASCULLI, *Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali*, op .cit., p. 116, in cui l'autore spiega che le misure di prevenzione possono senz'altro consistere in *best practices*. Queste, in particolare, si sostanziano in comportamenti adottati da imprese, pubblici uffici e professionisti in attuazione di regolamenti settoriali. Più precisamente le *best practices* rientrano nel cosiddetto modello situazionale della prevenzione positiva, di cui si parlerà più diffusamente nel prosieguo del Capitolo.

aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali», con la precisazione che esso deve essere commesso per via telematica (*rectius* cibernetica) [436] e, per quanto attiene ai soggetti passivi, ai danni di minori[437].

Sotto il profilo psicologico, invece, l'art. 1, co. 2, l. 71/2017 richiede che il *cyberbullo* agisca con lo scopo intenzionale e predominante di «*isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo*»[438].

Orbene, diversamente dal cyberterrorismo – che, del pari, non ha ricevuto autonoma tipizzazione -, il legislatore ha ritenuto opportuno intervenire in materia di cyberbullismo con un apposito provvedimento a vocazione preventiva – atteso, da un lato, il connotato cibernetico del comportamento rilevante e, dall'altro lato, l'età dei soggetti coinvolti e l'importanza dei beni giuridici di cui essi sono titolari - e con una *strategia di attenzione*, *tutela* ed *educazione* nei confronti dei minori (art. 1, co. 1, l. 71/2017)[439].

---

[436] Sul punto è interessante notare come il legislatore del 2017 abbia aggiornato il proprio vocabolario giuridico, preferendo impiegare, nell'art. 1 della l. 71/2017, la dizione «*via telematica*» in luogo di quella tradizionale «*via informatica*».

[437] Per un esame dei profili penalmente rilevanti del cyberbullismo si veda C. GRANDI, *Le conseguenze penalistiche delle condotte di cyberbullismo. Un'analisi de jure condito*, in *Annali online della Didattica e della Formazione Docente*, Vol. 9, n. 13/2017, pp. 40-58. Per un esame approfondito dei reati che rilevano in ordine alla manifestazione del cyberbullismo V. SELLAROLI, *Il nuovo reato di cyberbullismo (l. 29 maggio 2017, n. 71)*, op. cit., pp. 13 e ss.

[438] V. SELLAROLI, *Il nuovo reato di cyberbullismo (l. 29 maggio 2017, n. 71)*, op. cit., pp. 30 e ss., in cui l'autrice aggiunge che: «qualsiasi condotta – anche grave – che non assuma la finalità di isolare dovrebbe essere esclusa dall'ambito di applicazione della legge. La distinzione in alcuni casi potrebbe non essere d'immediata percepibilità, considerando che intenzionalità e prevalenza sono indicati in termini cumulativi e non alternativi». Con riguardo all'atteggiamento psicologico, dunque, il cyberbullo deve agire con lo «scopo intenzionale e predominante di isolare un minore o un gruppo di minori». Detta peculiare finalità rappresenta l'elemento che distingue la «*non fattispecie*» di cyberbullismo dalle fattispecie che, *ex* art. 1, co. 2, possono rilevare ai fini della sua manifestazione.

[439] Sulla *ratio* preventiva della legge 71/2017 si veda V. SELLAROLI, *Il nuovo reato di cyberbullismo (l. 29 maggio 2017, n. 71)*, op. cit., pp. 10 e ss., in cui l'autrice spiega che: «Le novità introdotte dalla legge in questione, si basano anzitutto sulla cifra fondamentale della prevenzione di un fenomeno che presenta moltissimi segnali premonitori e condotte di segno

Tra le misure più significative introdotte dal legislatore merita attenzione l'istituzione - senza nuovi o maggiori oneri per la finanza pubblica – del «tavolo tecnico per la prevenzione e il contrasto del cyberbullismo». L'organo, istituito presso la Presidenza del Consiglio dei Ministri e composto dai rappresentanti dei soggetti coinvolti a vario titolo in materia[440], è incaricato di redigere il «piano di azione integrato per il contrasto e la prevenzione del cyberbullismo», da completare con il «codice di coregolamentazione per la prevenzione e il contrasto del cyberbullismo» (art. 3, co. 3).

Detti strumenti, a norma dell'art. 3, co. 3, l. 71/2017, si rivolgono agli operatori della rete internet e, precipuamente, ai fornitori dei servizi di *social networking*. La previsione in parola conferma come le piattaforme *social* siano strumenti che - mettendo in relazione un numero potenzialmente infinito di utenti - sono in grado di amplificare la pervasività delle condotte dei reati cibernetici, imponendosi nell'attuale scenario delle comunicazioni come il luogo virtuale idealtipico per la commissione dei fatti di cyberbullismo e cyberterrorismo[441].

Altro aspetto rilevante della disciplina dettata dalla l. 71/2017 è la preferenza accordata dal legislatore alle *misure di prevenzione positiva*. Trattasi di strumenti che, anziché limitare la libertà del proposto, intervengono con iniziative

---

apparentemente neutro. […] La prevenzione, primaria e secondaria, si rivolge proprio nello specifico a quei comportamenti che non sono reato (e che non è il caso che lo diventino) ma che, ciò nonostante, creano profondo disagio e sofferenza nella vittima e, se non affrontati precocemente, si trasformeranno, verosimilmente presto, in violazione di una norma penale».

[440] Al «*tavolo tecnico per la prevenzione e il contrasto del cyberbullismo*» partecipano, a norma dell'art. 3, co. 1, d.lgs. 232/2011, i rappresentanti dei Ministeri di Interno, Istruzione, Università e Ricerca, Lavoro e Politiche Sociali, Giustizia, Sviluppo economico, Salute, i rappresentanti della *Conferenza unificata* (art. 8 d.lgs. 28.8.1997, n. 281), *dell'Autorità per le garanzie nelle comunicazioni*, del *Garante per l'infanzia e l'adolescenza*, del *Comitato di applicazione del codice di autoregolamentazione media e minori*, del *Garante per la protezione dei dati personali*, di associazioni con comprovata esperienza nella promozione dei diritti dei minori e degli adolescenti e nelle tematiche di genere, degli operatori che forniscono servizi di *social networking* e degli altri operatori della rete internet, delle associazioni studentesche e dei genitori e, infine, delle associazioni attive nel contrasto del bullismo e del cyberbullismo.

[441] Per un esame del ruolo dei *social networks* rispetto ai *cybercrimes* si rinvia a C. D'ONOFRIO, *Il cyberbullismo*, in F. CORONA (a cura di), *Reati informatici e investigazioni digitali. Diffamazione via web – Prove digitali – Sex crimes – Cyberstalking – Cyberbullismo – Reati privacy*, Pacini Giuridica, pp. 169 e ss.

di tipo prettamente sociale e culturale rivolte ai consociati - in questo caso minori – al fine di fornirgli strumenti educativi utili ad evitare che essi si determinino a commettere reati in futuro[442]. Il ricorso alle misure di prevenzione positiva rappresenta una novità assoluta per il nostro ordinamento, il quale tradizionalmente, come si è detto, ha impiegato esclusivamente *misure di prevenzione negativa*.

La nuova strategia - che persegue la funzione general e special preventiva attraverso *misure di prevenzione*, anziché attraverso fattispecie di reato - pare confermare che il legislatore italiano ha finalmente compreso l'inefficacia della rigida applicazione dello strumento penale in funzione prevenzionistica dei reati cibernetici. In materia devono infatti preferirsi misure più flessibili, che, nel rispetto delle garanzie costituzionali elaborate dalla giurisprudenza, consentano di intervenire sul sostrato culturale che è elemento essenziale e costitutivo dei nuovi reati.

Tra le misure di prevenzione positiva più rilevanti contro il cyberbullismo, l'art. 3, co. 5, l. 71/2017 prevede che la Presidenza del Consiglio dei Ministri predisponga periodiche campagne informative di prevenzione e di sensibilizzazione sul fenomeno criminoso in parola, avvalendosi dei principali media e degli organi di comunicazione e di stampa[443].

---

[442] L. PASCULLI, *Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali*, op. cit., p. 112, in cui l'autore evidenzia che tra le misure di prevenzione positiva di tipo sociale figura il *Developmental crime prevention* (o *prevenzione evolutiva*). Esso consiste nell'offrire ai giovani e in particolare ai minori opportunità parasociali precoci «che consentano di individuare tempestivamente e rimuovere fattori criminogeni o correggere tendenze antisociali, prima che possano sfociare in un comportamento criminoso (early intervention)». L'idea di fondo della prevenzione evolutiva è che il modo migliore per prevenire la criminalità, anche tra gli adulti, sia quello di favorire un ottimale sviluppo della personalità dei minori. Nello stesso senso S. P. LAB, *Crime Prevention. Approaches, Practices, and Evaluations*, Taylor & Francis, 2013, pp. 157 e ss.; B. C. WELSH, D. P. FARRINGTON, *The Oxford Handbook of Crime Prevention*, Oxford University Press, 2014, pp. 8-9.

[443] L'art. 3, co. 5, l. 71/2017 prevede che la Presidenza del Consiglio dei Ministri organizzi le campagne informative di prevenzione e di sensibilizzazione sul cyberbullismo di concerto con i Ministeri dell'Istruzione, dell'Università e della Ricerca e con l'Autorità per le garanzie nelle comunicazioni.

A norma dell'art. 4, co. 1, l. 71/2017, poi, il Ministero dell'Istruzione, dell'Università e della Ricerca, sentito il Dipartimento per la giustizia minorile e di comunità del Ministero della Giustizia, è tenuto ad elaborare, con la collaborazione della Polizia postale, *linee di orientamento* per la *prevenzione ed il contrasto del cyberbullismo* nelle scuole. In particolare, le linee di orientamento includono la formazione del personale scolastico, con l'individuazione di un referente per ogni istituto d'istruzione; la promozione di un ruolo attivo degli stessi studenti nella prevenzione e nel contrasto del cyberbullismo nelle scuole; la previsione di misure di sostegno e rieducazione dei minori coinvolti (art. 4, co. 2, l. 71/2017). In altri termini la legge 71/2017 prevede che gli istituti scolastici, quali enti pubblici dedicati all'istruzione, si muniscano di una sorta di *modello* - con l'individuazione di un coordinatore che vigili sulla sua attuazione – per la prevenzione ed il contrasto del cyberbullismo.

L'art. 4, co. 4 della legge in esame, inoltre, prevede che gli uffici scolastici regionali promuovano la pubblicazione di bandi per il finanziamento di progetti di particolare interesse, elaborati da reti di scuole e finalizzati a promuovere azioni integrate di contrasto del cyberbullismo e l'educazione alla legalità[444].

Ad ogni buon conto, conformemente a quanto previsto in via generale dal *Cybersecurity Act*, la prevenzione dei *cybercrimes* presuppone indispensabilmente un processo di *alfabetizzazione cibernetica*. Questa, come chiarito nel precedente Capitolo del presente lavoro, consiste in un vero e proprio processo formativo e culturale, che quindi rientra a pieno titolo tra le *misure di prevenzione positiva*. Il fondamento normativo dell'*alfabetizzazione cibernetica* in materia di cyberbullismo si rinviene nell'art. 4, co. 5, l. 71/2017, che prevede che le istituzioni scolastiche siano tenute a promuovere l'educazione «all'uso consapevole della rete internet e ai diritti e doveri connessi all'utilizzo delle

---

[444] Le iniziative che prevendo l'elaborazione dei bandi ed il finanziamento dei progetti relativi alla prevenzione ed al contrasto del cyberbullismo non sono prerogativa esclusiva degli Istituti scolatici. Invero questi, per la loro redazione, si avvalgono della collaborazione degli enti pubblici e privati a vario titolo coinvolti nel settore ed in particolare: i servizi minorili dell'Amministrazione della giustizia, le Prefetture, gli enti locali, i servizi territoriali, le forze di polizia, nonché le associazioni private (art. 4, co. 4, l. 71/2017).

tecnologie informatiche». Tale insegnamento, che è trasversale rispetto alle diverse discipline curricolari, include la realizzazione di apposite attività progettuali, promosse da reti di scuole in collaborazione con enti locali, servizi territoriali, organi di polizia, associazioni ed enti.

Nonostante nella l. 71/2017 il legislatore, in attuazione delle previsioni eurounitarie in materia di prevenzione dei *cybercrimes*, abbia ritenuto di prediligere – in via del tutto inedita – le predette misure positive per la prevenzione del cyberbullismo, l'art. 7 della stessa ammette il ricorso all'*ammonimento* (che è la misura di *prevenzione negativa* più tenue nota al nostro ordinamento), istituendo una sorta di "*doppio binario*" fra misure positive e negative.

Trattasi di una misura questorile, che può essere applicata fintantoché non intervenga la querela della persona offesa o la denuncia per taluno dei reati di cui agli artt. 594, 595 e 612 c.p. e 167, d.lgs. 30.6.2003, n. 196, qualora le condotte vengano poste in essere, mediante l'uso di internet, da parte di un minore infraquattordicenne ai danni di un altro minore.

Quanto al contenuto, la misura consiste in un "comando" a carico del prevenuto, che rimane in ogni caso libero di aderirvi o meno, senza che a ciò consegua una sanzione penale. Tutt'al più l'ammonimento può comportare il mutamento della *procedibilità* per l'eventuale reato che il prevenuto commetta sotto la vigenza della misura, non richiedendosi, in tal caso, la querela della persona offesa ma bastando la denuncia[445].

---

[445] Per un esame delle misure dell'ammonimento e della sua disciplina in generale, F. MENDITTO, *Le misure di prevenzione*, op. cit., pp. 261 e ss., in cui si spiega che la misura, avente natura amministrativa, viene impiegata elettivamente per prevenire il delitto di "*Atti persecutori*" (art. 612-*bis* c.p.), che certamente può integrare una delle forme di manifestazione del cyberbullismo. L'ammonimento non richiede la previa commissione del reato, ma l'esistenza di comportamenti la cui reiterazione comporterebbe più gravi condotte costituenti reato. Quanto al contenuto, la misura consiste nell'invito a tenere una condotta conforme alla legge, inducendo l'interessato alla riflessione e al ravvedimento, prima che l'aggravamento sfoci nell'attivazione del procedimento penale. Giova osservare che recentemente la Terza Sezione del Consiglio di Stato, con sentenza del 21.4.2020, n. 2545, si è pronunciata in materia, statuendo che: «Lo strumento dell'ammonimento è essenzialmente destinato a prevenire la recrudescenza dei fenomeni patologici talvolta caratterizzanti le relazioni umane, anche di impronta affettiva, laddove una delle

L'art. 2, l. 71/2017, rubricato "*Tutela della dignità del minore*", prevede le ulteriori misure dell'*oscuramento*, della *rimozione* e del *blocco*, le quali - diversamente dall'ammonimento - non vengono impiegate in funzione preventiva *strictu sensu*, rispondendo – pur non essendo pene accessorie irrogate all'esito di un processo penale - all'esigenza di evitare la reiterazione delle condotte *ex* art. 1, co. 2[446]. Le misure in questione possono essere richieste da parte del minore, se ultraquattordicenne (o da ciascun genitore o soggetto esercente la responsabilità sullo stesso se infraquattordicenne), direttamente al titolare del trattamento o al gestore del sito internet o del *social media*, ove siano stati posti in essere i comportamenti rilevanti a norma dell'art. 1, l. 71/2017.

Sulla scorta delle considerazioni svolte con riguardo al cyberbullismo, pare potersi affermare che il legislatore abbia finalmente compreso che per contrastare efficacemente i *cybercrimes*, specie quelli più ignobili (in ragione dei beni giuridici offesi) ed insidiosi (per le modalità esecutive della condotta), è quanto mai opportuno adottare una strategia ispirata alla *prevenzione*. Tuttavia, differentemente dall'impostazione tradizionale, la prevenzione dei reati cibernetici non può attuarsi attraverso una scriteriata proliferazione di nuove fattispecie di reato, connotate dall'anticipazione della soglia della rilevanza penale - mediante l'impiego di tecniche di incriminazione frutto dell'accostamento abnorme di istituti del diritto penale quali, ad esempio, la struttura del reato di pericolo ed il

---

parti assuma atteggiamenti di prevaricazione ed indebita ingerenza nella sfera morale dell'altra». Tali previsioni generali valgono anche per l'ammonimento in materia di cyberbullismo, rispetto al quale l'art. 7, co. 2, l. 71/2017 prevede una disciplina con alcuni profili di specialità, legati all'età dei soggetti coinvolti. Invero, per l'applicazione dell'ammonimento, il questore convoca il minore prevenuto unitamente ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale. Al compimento della maggiore età del prevenuto gli effetti della misura cessano.

[446] Per un approfondito esame delle misure di *oscuramento, rimozione e blocco* in materia di cyberbullismo (le seconde due, come si ricorderà, erano previste anche dal legislatore europeo in materia di terrorismo *online* nel regolamento 2021/784 e nella direttiva 2017/541) si rinvia a B. G. BELLO, L. SCUDIERI, *L'odio online: forme, prevenzione e contrasto*, Giappichelli, 2022, pp. 128 e ss. In riferimento alle misure in parola si precisa che sono dei rimedi a carattere amministrativo «ascrivibili alle procedure c.d. *notice* e *takedown* che si caratterizzano per la semplicità della richiesta e la tempestività della risposta». Inoltre, si osserva criticamente che il testo dell'art. 2, l. 71/2017 sarebbe affetto da indeterminatezza in quanto indica come oggetto delle misure in questione «qualsiasi altro dato del minore», senza ulteriori specificazioni.

dolo specifico - in spregio ai principi costituzionali. Invero devono preferirsi le misure di prevenzione ed in particolare quelle di tipo positivo.

Per tali ragioni, si ritiene opportuno che il legislatore italiano adotti - nella perdurante mancanza di un'autonoma fattispecie di reato - un provvedimento per il contrasto e la prevenzione del cyberterrorismo, che presenta criticità di fondo consustanziali analoghe a quelle che affliggono il cyberbullismo, con il coinvolgimento di soggetti passivi e l'offesa di beni giuridici particolarmente rilevanti. L'intervento in materia dovrà conformarsi al diritto eurounitario, che, per il contrasto dei *cybercrimes*, attribuisce rilevanza strategica alla *positive prevention*, rispettando i principi dettatati dalla giurisprudenza domestica e ispirandosi, per quanto possibile, ai modelli già elaborati dalla legislazione speciale e militare.

5.3. Le misure di prevenzione positiva. In particolare i modelli di positive prevention sociale e situazionale

Con l'espressione *prevenzione positiva* si intende quel complesso di misure di carattere non coercitivo, consistenti generalmente in un incremento della sfera giuridica personale e in interventi di promozione di un maggior benessere individuale e sociale. Esse possono consistere in programmi socioassistenziali, programmi di formazione, modelli di prevenzione, premi e incentivi volti a promuovere il rispetto della legalità (e in particolare della legge penale) o anche in mezzi di difesa e di controllo volti a scoraggiare o a rendere più difficile la commissione di reati. Quando attengono all'individuo, tali misure ne promuovono l'inserimento nella società, che sarà tanto più agevole quanto più spontanea sarà l'adesione dell'interessato agli strumenti in parola[447].

---

[447] L. PASCULLI, *Le misure di prevenzione del terrorismo*, op. cit., pp. 103-104. In particolare, con riferimento alla funzione di reinserimento sociale delle misure di prevenzione, F. MERUSI, *Profili amministrativi delle misure di prevenzione*, in *Centro nazionale di prevenzione e difesa sociale*, *Le misure di prevenzione*, Atti del Convegno «Enrico De Nicola» (Alghero, 26-28

L'elemento che distingue le misure di *prevenzione negativa* da quelle di *prevenzione positiva* è dunque rappresentato dal contenuto coercitivo e restrittivo della libertà personale, che è proprio delle prime[448].

Autorevole dottrina ritiene che la prevenzione positiva *ante delictum* sia il modello da preferire per il contrasto del cyberterrorismo, come confermato dalla legislazione europea in materia di *cybercrimes* e di terrorismo *online* esaminata e dall'uso che i Paesi di *common law* già ne fanno, considerandolo il modello di prevenzione del crimine per antonomasia[449].

---

arile 1974), Giuffrè, 1975, p. 121. In senso parzialmente contrario cfr. I. SEREDYŃSKA, *Insider Dealing and Criminal Law. Dangerous Liaisons,* Springer Berlin Heidelberg, 2011, pp. 173 e ss., in cui l'autrice ritiene che la prevenzione positiva possa essere esclusivamente di tipo generale e che possa essere impiegata solo come complemento rispetto ad altre forme di deterrenza, da usare in via principale. L'autrice precisa altresì che: «[…] the positive prevention theory insists on the creation of such a social model of behaviour that does not take into account the commission of an offence» e che, per questa ragione, la positive prevention può essere definita «educative deterrence»

[448] Sulla distinzione fra misure di prevenzione *negativa* e *positiva* si veda P. NUVOLONE, *Relazione introduttiva, in Centro nazionale di prevenzione e difesa sociale*, *Le misure di prevenzione*, Atti del Convegno «Enrico De Nicola» (Alghero, 26-28 aprile 1974), Giuffrè, 1975, pp. 18-19; F. MERUSI, *Profili amministrativi delle misure di prevenzione*, op. cit., pp. 137 e ss.; R. GUERRINI, L. MAZZA, S. RIONDATO, *Le misure di prevenzione. Profili sostanziali e processuali*, op. cit., pp. 8-10; N. BOBBIO, voce «*Sanzione*», in *Nov. Dig. It.*, XVI, UTET, 1969, p. 531.

[449] L. PASCULLI, *Le misure di prevenzione del terrorismo*, op. cit., p. 16, in cui l'autore osserva che: «Generalmente, nei paesi di *common law*, come il Regno Unito o gli Stati Uniti d'America, esistono provvedimenti assimilabili alle nostre misure preventive, benché letteralmente le misure di *crime prevention* siano misure positive che mirano a prevenire il crimine mediante la riduzione delle occasioni di delinquenza e la promozione dell'integrazione sociale e del benessere individuale e sociale. Non vi è afflittività nei loro contenuti. Esse piuttosto sviluppano e favoriscono (o, per lo meno, non comprimono) la personalità dell'individuo». L'autore, inoltre, propone una distinzione, in relazione all'utilizzo dei modelli di prevenzione, fondata su un criterio "geografico", anziché sulla natura degli ordinamenti. Invero sarebbe possibile distinguere fra Paesi, come quelli nordeuropei, che prediligono ampi interventi sociali e di *welfare* o interventi specialpreventivi comunque ispirati a ragioni terapeutiche, umanitarie e assistenziali più che neutralizzanti (c.d. «modello nordico») e Paesi che, invece, in aggiunta a (o al posto di) una prevenzione positiva, non rinunciano a modelli di prevenzione speciale più invasivi per la libertà del singolo, se non addirittura coercitivi. Nel secondo gruppo rientrano sia Paesi di *common law* che Pesi di *civil law*. I primi riconducono le misure di prevenzione positiva entro il proprio arsenale giuspenalistico, mentre i secondi le collocano nel novero degli strumenti amministrativi (ivi, p. 58). Per un esame del cosiddetto «*modello nordico*», nel quale la *crime prevention* coincide con la *positive prevention*, si rinvia a H. TAKALA, *Nordic Cooperation in Criminal Policy and*

La dottrina ha elaborato due diversi modelli di prevenzione positiva.

Il primo modello, detto di *prevenzione sociale*, prevede il compimento di azioni di sviluppo della società, che siano in grado di incidere direttamente sulle cause, sugli elementi o sui processi criminogeni[450].

La prevenzione sociale, a sua volta, si articola in numerosi *sottomodelli* - dei quali si ritiene opportuno esaminare brevemente i più rilevanti - che si distinguono in base ai gruppi di consociati o agli elementi della società rispetto ai quali si rivolgono.

Il *Community development model* (*o community-based prevention* o *community programs*) si fonda sulla convinzione che il crimine abbia causa non solo o non tanto nella predisposizione alla delinquenza del singolo soggetto (ovverosia la sua pericolosità sociale), bensì anche e soprattutto in una serie di altri fattori relativi all'ambiente sociale specifico di certe comunità. Il sottomodello prevede la predisposizione di programmi volti a rivitalizzare e a supportare le istituzioni locali di tali comunità, tramite finanziamenti statali volti a sostenere specifiche iniziative o tramite l'istituzione di comitati su base locale, gestiti dalle forze di polizia o, comunque, da personale appositamente formato, con il compito di porre in essere interventi di miglioramento delle condizioni sociali delle singole aree interessate[451].

Crime Prevention, in *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 5/2004, pp. 131 e ss..

[450] Per la definizione di *prevenzione sociale* ed un'analisi delle sue origini e dei suoi sviluppi H. GRANT, *Social Crime Prevention in the Developing World Exploring the Role of Police in Crime Prevention*, Springer, 2014, pp. 3-4: «In sum, social crime prevention or "crime prevention through social development" (Pelser 2002) is a strategy which favors the struggle against the underlying causes of criminal activity and victimization. It will be argued that CPSD holds the only sustainable potential of preventing crime in developing countries. Additionally, given that they are likely to be the most effective in the long-term, social crime prevention approaches should not be seen as "soft" approaches».

[451] Cfr. S. SCHNEIDER, *Crime Prevention. Theory and Practice*, Taylor & Francis, 2014, p. 242: «The community development model promotes the physical, social, and socioeconomic development of a neighborhood, which includes a range of initiatives from organizing residents, economic development, beautification projects, graffiti removal, housing gentrification, and other types of physical development. Social problem-solving approaches […] that address the root causes of crime through the development of local social cohesion and informal social control, and through social and economic development measures that address

Il *Development crime prevention* (o prevenzione evolutiva), invece, consiste nell'offrire ai giovani e, in particolare, ai minori opportunità parasociali e percorsi che consentono di individuare tempestivamente e rimuovere fattori criminogeni o correggere tendenze antisociali, prima che possano sfociare in un comportamento criminoso[452].

Il *Neighbourhood watch*, infine, consiste in programmi che promuovono l'attiva collaborazione dei cittadini nel controllo del crimine da parte delle forze dell'ordine, tramite attività di vigilanza e di denuncia[453]. Usualmente tali programmi si inseriscono nell'ambito di più ampie iniziative, contribuendo alla formazione di un nesso fra i due modelli di prevenzione positiva (sociale e situazionale)[454].

Il secondo modello, invece, è detto di *prevenzione situazionale* e consiste in tutta una serie di misure volte a ridurre le opportunità di commissione di reati, mediante interventi sull'ambiente fisico o attraverso l'intensificazione del controllo sociale o, ancora, mediante il rafforzamento delle difese delle potenziali

---

criminogenic risk factors»; B.C. WELSH, A. HOSHI, *Communities and crime prevention*, in D.P. FARRINGTON, L.W. SHERMAN, B.C. WELSH, D.L. Mackenzie, *Evidence-based Crime prevention*, Routledge, 2002, p. 165 e ss.; T. HOPE, *Community Crime Prevention*, in D.P. FARRINGTON, M. TONRY, *Building a Safer Society*, *Strategy Approaches to Crime Prevention*, University of Chicago Press, 1995, p. 21 ss.

[452] S. N. ZANE, B. C. WELSH, G. M. ZIMMERMAN, *Examining the Historical Developments and Contemporary Relevance of the Longitudinal–Experimental Design of the Cambridge-Somerville Youth Study: Utility for Research on Intergenerational Transmission of Offending*, Springer International Publishing, 2016, p. 1: «Developmental crime prevention refers to interventions designed to prevent the development of criminal potential in individuals (Tremblay and Craig 1995). It can be contrasted with situational crime prevention - interventions designed to prevent the occurrence of crimes by reducing opportunities and increasing the risk and difficulty of offending (Smith and Clarke 2012) - and community prevention - interventions designed to change the social conditions and institutions that influence offending in residential communities (Hope 1995)»; R. HOMEL, *Developmental Crime Prevention*, in N. TILLEY, *Handbook of Crime Prevention and Security Safety*, Willan Publishing, 2005, p. 71 ss.

[453] Sull'interazione tra cittadino e polizia, come misura di *Neighbourhood Watch*, si veda F. LAMERIS, *Crime Control: A Proposal for The Netherlands*, in *Police Stud. Int'l Rev. Police Dev*., 6/1983-1984, pp. 13 e ss.

[454] K. PERRY, *Measuring the Effect of Neighbourhood Crime Watch in Lakewood*, *Colorado*, in *Police J*., 57, 1984, pp. 221 e ss.; J. H. HENDERSON, *Public Law Enforcement, Private Security and Citizen Crime Prevention: Competition or Cooperation*, in *Police J.*, 60, 1987, p. 48.

vittime[455]. La *ratio* degli interventi preventivi situazionali è dunque triplice rispetto alla commissione del reato: a) ridurne le opportunità; b) aumentarne i rischi e i costi; c) ridurne la convenienza ed il profitto[456].

Quanto alla natura, le misure di prevenzione situazionale possono atteggiarsi variamente. Esse, ad esempio, possono consistere in banali accorgimenti, quali nascondere gli oggetti di valore, impiegare dispositivi di sicurezza (quali lucchetti, serrature, vetri antisfondamento, sistemi antifurto, servizi di vigilanza privata) e, in *ambito cibernetico*, sistemi di controllo degli accessi ai sistemi di informazione (come *passwords*, autenticazione a più fattori ecc.). Altri esempi di prevenzione situazionale sono la registrazione dei beni patrimoniali, la tenuta di registri e di rapporti, nonché la conservazione di informazioni bancarie precipuamente a fini di antiriciclaggio. Al medesimo modello appartengono anche i codici comportamentali, quelli di condotta, i regolamenti, le *best pratices*, nonché i *modelli* di organizzazione-gestione-controllo, che, come si è visto, possono essere adottati dalle persone giuridiche[457].

---

[455] Per una definizione della *prevenzione situazionale* ed un esame delle sue origini e dei suoi sviluppi si rinvia a A. WAKEFIELD, A. VON HIRSCH, D. GARLAND, *Ethical and Social Perspectives on situational Crime Prevention*, Bloomsbury Academic, 2000, pp. 1 e ss., in cui l'autore evidenzia che: «Situational crime prevention (SCP) is a set of recipes for steering and channeling behaviour in ways that reduce the occurrence of criminal events. Its project is to use situational stimuli to guide conduct towards lawful outcomes, preferably in ways that are unobtrusive and invisible to those whose conduct is affected».

[456] L. PASCULLI, *Le misure di prevenzione del terrorismo*, op. cit., p. 115; P.L. BRANTINGHAM, P.J. BRANTINGHAM, W. TAYLOR, *Situational Crime Prevention as a Key Component in Embedded Crime Prevention*, in *Canadian J. Criminology & Crim. Just*., n. 47, 2005, p. 276, in cui gli autori, oltre alle funzioni menzionate, ne individuano di ulteriori, ovverosia: la *riduzione della provocazione al reato* e la *riduzione della possibilità di addurre scuse a propria giustificazione*.

[457] Per una panoramica dei dispositivi di prevenzione situazionale si rinvia a R.V. CLARKE, *Situational Crime Prevention*, in *Crime & Just*., 19, 1995, p. 91.

6. Le misure di prevenzione positiva contro il cyberterrorismo. Osservazioni conclusive

Alla luce delle considerazioni sinora svolte con riguardo alle misure di prevenzione positiva in generale, è ora necessario vagliare l'applicabilità delle stesse al cyberterrorismo.

Sul punto rileva preliminarmente ricordare che il fenomeno in questione non può essere trattato come la mera giustapposizione del terrorismo, da un lato, e del *cybercrime*, dall'altro. Infatti, come si è detto, le componenti essenziali caratteristiche dell'uno e dell'altro fenomeno si fondono inscindibilmente nel cyberterrorismo, contribuendo a connotarlo di forza e pervasività - verso i nuovi beni giuridici offesi - notevolmente accresciute rispetto a quelle dei due reati che concorrono ad integrarne il fatto tipico[458]. Per tali ragioni, le misure di prevenzione, volte ad assicurare un efficace contrasto del fenomeno, devono tenere conto delle suddette componenti. Queste ultime, come emerso nei precedenti Capitoli I e II, sono, da un lato, il binomio *natura-contesto,* relativo alle condotte terroristiche (art. 1 della decisione-quadro 2002/475/GAI) e, dall'altro lato, il *cyberspace*, come *locus commissi delicti* virtuale, difficilmente inquadrabile entro le categorie tradizionali del diritto penale.

Orbene, in relazione alla prima componente, le *misure di prevenzione positiva* intervengono direttamente sui presupposti sociali, culturali, politici ed ambientali dei comportamenti umani, attraverso azioni che, lungi dal risolversi in una mera compressione della libertà dei soggetti, rispondono alla *ratio* di contribuire alla loro formazione, al fine di evitare che essi accolgano ideologie estremistiche - subdolamente propagandate in rete e nei *social networks* - e, quindi, si determinino a commettere reati di cyberterrorismo.

Più specificamente la formazione in parola deve consistere in un processo di *alfabetizzazione cibernetica*, che, attraverso strumenti di crescita culturale e

---

[458] C. LAMBERTI, *Gli strumenti di contrasto al terrorismo ed al cyber-terrorismo nel contesto europeo*, op. cit., pp. 142 e ss.

sociale - attivati da parte dello Stato - contribuisca a sviluppare il pensiero critico dei consociati, per un utilizzo ragionato delle tecnologie cibernetiche, al fine di evitare condizionamenti peculiarmente in ambito politico, rilevanti rispetto alla finalità cyberterroristica.

Sul punto, solo a titolo esemplificativo, si potrebbe pensare ad un efficientamento dei presidi scolastici nelle aree maggiormente esposte al rischio che i minori - la cui fiducia può essere facilmente carpita attraverso artifici, raggiri e minacce posti in essere nell'Internet e nei *social networks* - cedano alle lusinghe dei gruppi terroristici, che cercano di indottrinarli sin dall'età infantile; all'organizzazione, da parte delle Istituzioni governative competenti, di corsi o iniziative culturali - con la partecipazione di esperti provenienti dalla società civile - volti ad educare i cittadini alla legalità; all'avvio di percorsi formativi che forniscano ai consociati gli strumenti per approcciarsi in modo critico all'utilizzo di *Internet* e dei *social networks*, verificando le informazioni ivi reperibili. Tali iniziative eleverebbero socialmente e culturalmente i consociati (specie i minori), permettendogli di compiere scelte consapevoli ed informate, con l'effetto di indebolire l'opera dei cyberterroristi, volta a condizionarne le scelte politiche.

Quanto alla componente del *cyberspace*, invece, le misure di prevenzione si rivelano gli strumenti più adatti a contrastare il cyberterrorismo in ragione della loro *flessibilità applicativa*[459]. Infatti, come si è detto in via generale, esse non richiedono prove *strictu sensu*, bensì indizi (purché corredati da adeguati riscontri

---

[459] Sul punto si veda Sistema di Informazione per la Sicurezza della Repubblica (SISR), *Relazione annuale sulla politica dell'informazione per la sicurezza*, cit., p. 84, in cui si legge: «L'attività di contrasto condotta nei Paesi europei nel corso del 2021 ha fornito ulteriori elementi utili a meglio definire il profilo di soggetti estremisti/radicalizzati, coinvolti, in taluni casi, nella pianificazione di atti ostili. Tratti comuni a molti di questi individui sono la giovane età (anche minorenni) e una condizione di marginalità economico-sociale. In questo contesto, i social media si confermano gli ambienti d'elezione dove i giovani *homegrown* consumano propaganda, reperiscono "guide" per l'auto-addestramento con finalità offensive e intessono rapporti con correligionari di analogo orientamento. L'impegno informativo si è focalizzato pertanto sulla minaccia rappresentata anche da micro-gruppi o circuiti più ampi e transnazionali, composti tendenzialmente da elementi radicalizzati attivi online e in contatto fra loro soprattutto tramite i *social networks*. In tal senso, gli ambienti virtuali hanno avuto un effetto aggregante rispetto a comunità distinte e/o frammentate, le cui differenze linguistiche, culturali ed etniche avevano finora impedito qualsiasi commistione».

oggettivi), fermo in ogni caso il rispetto di tutte le stringenti garanzie indicate dalla giurisprudenza europea e nazionale (sostanzialmente analoghe a quelle previste per la materia penale). Tali elementi indiziari, che, come noto, consentono di fornire adeguati riscontri della probabilità che il proposto commetta il reato e dell'obiettiva rilevanza - rispetto alla commissione dello stesso - degli atti già compiuti, sono più agevolmente reperibili, specie in un luogo connotato da evidenti profili di criticità, quale è il *cyberspace*. Diversamente, la ricerca e la formazione della prova in ordine alla dimostrazione della penale responsabilità, nel caso di un capo di imputazione relativo ad una delle cosiddette fattispecie prevenzionistiche, rischierebbe, a causa della depersonalizzazione, deterritorializzazione e detemporalizzazione che connotano il *cyberpace*, di rendere intempestivo l'intervento penale, frustrando quindi ogni *ratio* preventiva.

Conclusivamente si osserva che le misure di prevenzione (negative e positive, da usare congiuntamente) sono gli strumenti giuridici elettivamente deputati a prevenire i reati di cyberterrorismo e devono preferirsi rispetto alle fattispecie di reato costruite mediante tecniche di incriminazione volte ad anticipare la rilevanza penale – anche oltre la soglia del tentativo punibile -, tanto da fare strame dei principi fondamentali del diritto penale costituzionale. L'utilizzo delle misure di prevenzione nel settore in parola è auspicato dalla stessa Unione Europea, che ha disciplinato la materia con la direttiva 2016/1148, da un lato, e con la direttiva 2017/541 ed il regolamento 2021/784, dall'altro lato, prediligendo misure di tipo positivo. Diversamente, l'ordinamento italiano ha sempre impiegato esclusivamente misure di prevenzione negativa, interrompendo la tradizione solo nel 2017, quando è entrata in vigore la legge sulla prevenzione del cyberbullismo (l. 71/2017). Questa, invero, ha previsto, per la prima volta, l'uso combinato di misure positive e negative, limitando le seconde al solo ammonimento.

Ad ogni buon conto, la preferenza da accordare alle misure di prevenzione non è legata esclusivamente alla proliferazione delle suddette fattispecie prevenzionistiche. Invero gli strumenti di *positive prevention* sono in grado di intervenire direttamente sugli elementi essenziali che connotano, sotto il profilo

oggettivo, il cyberterrorismo, ovverosia la *natura* ed il *contesto* delle condotte ed il *cyberspace*. Le misure in parola consistono in azioni di tipo sociale, culturale e politico, che non limitano la libertà personale dei consociati, ma, anzi, la ampliano, attraverso percorsi formativi che li educhino ad un utilizzo critico di *internet* e dei *social networks*, in modo tale da neutralizzare i fattori ambientali criminogeni che connotano il *cyberspace*.

La misura di prevenzione positiva di tipo sociale più emblematica in materia è la cosiddetta *alfabetizzazione cibernetica*. Trattasi di un processo culturale - che le Istituzioni europee e nazionali devono avviare a favore dei cittadini - il quale interviene sul *contesto* e sulla *natura* delle condotte poste in essere nel *cyberspace*, azzerando l'idoneità dei due fattori a rendere le stesse cyberterroristiche, secondo la versione aggiornata dell'art. 270-*sexies* c.p. che si è proposta.

CONCLUSIONI

Il diritto penale italiano non è ancora pronto a misurarsi con le sfide lanciate dalle tecnologie cibernetiche che hanno rivoluzionato profondamente i rapporti interumani nel corso dell'ultimo ventennio.

Il *cyberspazio* è il *non-luogo* ove la nuova socialità si manifesta. Trattasi dell'*infrastruttura strategica* composta da *physical layer, logical layer e human layer*, attraverso la quale lo Stato eroga servizi informativi essenziali in settori fondamentali ed esprime dunque la sua *personalità*. Tuttavia la struttura tradizionale dello Stato moderno entra in crisi in relazione allo spazio cibernetico. Questo, invero, non può essere perimetrato alla stregua del territorio e i cybernauti non costituiscono un popolo, con l'effetto di precludere l'operatività del paradigma della Sovranità.

L'assenza di un potere sovrano regolatore nel *cyberspace* rende indispensabile garantire adeguata tutela alle informazioni ivi trasferite e più in generale ai nuovi interessi giuridici emersi in relazione alla cibernetica, i quali non coincidono con l'inviolabilità del domicilio (alla quale si rivolge l'offesa dei cosiddetti *reati informatici* previsti dalla Sezione IV del Titolo XII del Libro II del codice penale).

In proposito il diritto eurounitario ha coniato il termine «*cybersicurezza*» per indicare l'insieme delle attività necessarie a proteggere la rete ed i sistemi informativi, gli utenti di tali sistemi e le altre persone interessate dalle minacce cibernetiche (art. 2, n. 1, regolamento 2019/881). La cybersicurezza è un bene pubblico da tutelare penalmente, che assomma in sé la *sicurezza* e la *riservatezza informatiche*, l'*habeas data* e l'*autodeterminazione informativa*. Quando la cybersicurezza riguarda le infrastrutture informative dello Stato, essa partecipa della sua *personalità*, siccome presidio di sicurezza nel *cyberspace*.

La crisi innescata dalla cibernetica involge le categorie del diritto penale tradizionalmente impiegate per determinare il *tempus* ed il *locus commissi delicti*. Con riguardo a quest'ultimo profilo, la Corte di Cassazione, pronunciandosi in

riferimento al delitto di *accesso abusivo ad un sistema telematico o informatico* (art. 615-*ter* c.p.), ha osservato come nel *cyberspace* - ove la condotta del reato perde concretezza sfumando in impulsi elettronici - rileva esclusivamente il luogo di partenza del dialogo tra i sistemi interconnessi e non invece la collocazione del sistema violato (Cass., SS.UU., sent. 24.4.2015, n. 17325).

Inoltre, la depersonalizzazione del *cyberspace* - ove è possibile operare in totale anonimato o avvalendosi di *fake profiles* - rende disagevole l'attribuibilità del fatto di reato all'agente, sia sotto il profilo oggettivo che soggettivo, con il rischio di precludere l'accertamento della responsabilità e, quindi, frustrare il rimprovero penale.

Le predette criticità evidenziano l'inadeguatezza delle *fattispecie informatiche* (o *computer crimes*) a tutelare efficacemente il bene della cybersicurezza e a descrivere le caratteristiche dei fatti commessi nello spazio cibernetico. Per tali ragioni si ritiene necessario introdurre nel codice penale la categoria dei *reati cibernetici* (o *cybercrimes*), i quali presuppongono, quale elemento essenziale del fatto tipico, il *cyberspace*, ove avvengono le condotte criminose. Rispetto all'integrazione dei nuovi reati, il computer ed il sistema informatico rappresentano null'altro che due dei possibili strumenti di cui il soggetto agente può avvalersi per "trasferirsi" dalla dimensione reale a quella virtuale e non, invece, l'oggetto materiale del reato né il bene giuridico da tutelare.

Sotto il profilo oggettivo, la condotta dei reati cibernetici consiste in comportamenti che rilevano in relazione a reati già previsti dal codice penale. A mero titolo esemplificativo si pensi al *cyberbullismo*, le cui condotte possono consistere in pressioni, aggressioni, molestie, ricatti, diffamazione, diffusione di contenuti *online* (art. 1, co. 2, l. 29.5.2017, n. 71). Sotto quello psicologico, invece, i *cybercrimes* si connotano per le specifiche finalità di volta in volta individuate dal legislatore. Nel caso del cyberbullismo, ad esempio, la finalità consiste alternativamente nell'isolare un minore (o un gruppo di minori), colpirlo con un attacco dannoso o metterlo in ridicolo.

Il cyberterrorismo è il *cybercrime politico* le cui condotte sono caratterizzate dalla finalità di terrorismo. La dottrina ha elaborato definizioni incomplete del fenomeno, che ne valorizzano gli aspetti tecnici ma tralasciano quelli giuridici, specie con riferimento alla componente terroristica.

Mancante un inquadramento giuridico del cyberterrorismo è prevalsa l'opzione di disciplinare il fenomeno attraverso la mera giustapposizione delle norme in materia di *reati informatici* e di *terrorismo comune*. Tuttavia siffatta scelta regolatrice non tiene conto delle peculiarità del fenomeno.

Sul punto giova osservare che - ferma la mancanza nel nostro ordinamento di una disciplina dei *cybercrimes* - l'art. 270-*sexies* c.p. fornisce la definizione di «*condotte con finalità di terrorismo*». La disposizione è il risultato di un processo di *eterointegrazione parziale* del diritto penale da parte di quello europeo, atteso che essa riproduce il contenuto dell'art. 1 della decisione-quadro 2002/475/GAI (rubricato "*Reati terroristici e diritti e principi giuridici fondamentali sulla lotta contro il terrorismo*"), purtuttavia rinunciando ad elencare le singole condotte rilevanti, che la norma europea, invece, tassativizza. Infatti l'art. 270-*sexies* c.p. attribuisce natura terroristica alle condotte in ragione delle finalità perseguite dal soggetto agente, che possono alternativamente consistere in: a) *intimidire la popolazione*; b) *costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto*; c) *destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale*.

Per quanto attiene ai requisiti oggettivi, invece, l'art. 270-*sexies* c.p. richiede che le condotte possano «*arrecare grave danno ad un Paese od a un'organizzazione internazionale*» per la loro «*natura*» o per il loro «*contesto*». I delitti terroristici devono dunque qualificarsi come *reati di pericolo concreto*, rendendosi necessario l'accertamento dell'*idoneità ad arrecare il grave danno*, attraverso il paradigma della prognosi postuma, sulla base dei criteri della «*natura*» e del «*contesto*». Più precisamente la *gravità* deve valutarsi in relazione all'intensità dell'offesa ed al carattere essenziale della struttura dello Stato presa di mira. Il concetto di *natura* si riferisce al tipo della condotta posta in essere, la

quale deve consistere in un comportamento potenzialmente rilevante rispetto a reati sufficientemente gravi (quali, ad esempio, la *strage*, il *naufragio, la sommersione, il disastro aviatorio* o *ferroviario*, l'*omicidio*, il *sequestro di persona, il danneggiamento*). Il *contesto*, infine, attiene alle circostanze di tipo *politico, sociale, culturale* in cui avviene la condotta. Esse potrebbero riguardare direttamente i *soggetti* coinvolti nel *reato* (si pensi, ad esempio, ad una particolare qualifica rivestita dal soggetto passivo o all'ideologia ed alla formazione culturale di quello attivo) o dei *fattori ambientali esterni* (ad esempio il sostrato culturale, sociale e ideologico di provenienza dall'agente).

La Corte di Cassazione ha esaminato i requisiti oggettivi delle condotte terroristiche ed i criteri da impiegare per la valutazione della loro idoneità offensiva, in relazione alla finalità più emblematica prevista dall'art. 270-*sexies* c.p., ovverosia la *costrizione dei* «*poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto*». In questo caso, secondo i giudici, l'idoneità della condotta ad arrecare grave danno al Paese deve essere valutata impiegando degli ulteriori criteri e precisamente: la «scala della decisione» potenzialmente imposta al potere pubblico; la «macrodimensione del fenomeno»; l'«illegittimità del metodo utilizzato per perseguire il fine di costrizione». Il sistema dei parametri giurisprudenziali consente di perimetrare l'ambito applicativo delle fattispecie di terrorismo – che non è un fenomeno squisitamente psicologico - ai soli fatti che, in concreto, possano arrecare grave danno al Paese, salvaguardando il principio di offensività.

Le considerazioni relative al *terrorismo comune* valgono anche per il cyberterrorismo, il quale, tuttavia, non è una mera forma di manifestazione del primo, attese le peculiarità che lo connotano sia dal punto di vista oggettivo che soggettivo.

Sotto il primo profilo, il cyberterrorismo richiede che le condotte avvengano nel *cyberspace*, il quale è elemento essenziale del fatto tipico del reato. Al contrario il *computer* rappresenta null'altro che uno dei possibili strumenti che il terrorista cibernetico può utilizzare per accedere al mondo virtuale.

Sotto il profilo psicologico, poi, le elaborazioni dottrinali e i più eclatanti fatti di cronaca (quale, ad esempio, il cosiddetto *Russiagate*) evidenziano come i cyberterroristi, oltre a perseguire gli scopi già tipizzati dall'art. 270-*sexies* c.p., possono subdolamente agire - specie abusando dei *social networks* (ad esempio utilizzando *fake profiles*, profilando gli utenti, postando messaggi propagandistici calibrati sui loro interessi) - per condizionare le scelte dei cittadini e, di riflesso, la Politica dello Stato, con violazione del metodo democratico costituzionale, che è l'essenza della sua *personalità*. Detta finalità, propria del solo cyberterrorismo, presuppone una *condotta violenta*, che nel *cyberspace* - abbandonate le armi da fuoco e gli esplosivi - assume natura *morale*. Essa può eventualmente ingenerare timore nella popolazione, qualora vengano strumentalmente prospettati esiti nefasti nel caso della mancata affermazione della linea politica sostenuta dai cyberterroristi.

Sulla scorta di tutte le predette considerazioni, si ritiene pertanto non ulteriormente procrastinabile l'introduzione di una fattispecie di reato nel codice penale che tenga conto di tutte le particolarità delle condotte cyberterroristiche, descrivendone adeguatamente i requisiti rilevanti in punto di idoneità offensiva e che tipicizzi il nuovo scopo.

La seconda parte della ricerca è stata dedicata all'esame degli strumenti per il contrasto del cyberterrorismo.

Il diritto europeo si occupa delle implicazioni giuridiche della cibernetica da oltre vent'anni. La Convezione di Budapest del Consiglio d'Europa sul *cybercrime* del 2001 ha previsto i reati di *accesso illegale ad un sistema informatico* (art. 2)*, intercettazione abusiva* (art. 3)*, attentato all'integrità dei dati* (art. 4) *e dei sistemi informatici* (art. 5) *e abuso di apparecchiature* (art. 6).

Alla Convenzione sono seguiti numerosi atti di diritto derivato - taluni estranei alla materia penale - con cui sono stati definiti concetti indispensabili per comprendere la portata del cyberterrorismo e approntare la strategia più efficace per il suo contrasto preventivo.

La direttiva 2013/40/UE è dedicata al contrasto degli attacchi ai sistemi di informazione impiegati nelle infrastrutture critiche dello Stato per l'esercizio delle

«*funzioni vitali della società*». La direttiva prescrive, da un lato, l'adozione di un approccio preventivo da attuare con misure che favoriscano il dialogo e lo scambio di informazioni tra soggetti pubblici e privati e, dall'altro, l'introduzione di nuove fattispecie di reato, tra le quali figurano l'*accesso illecito ai sistemi di informazione* (art. 3) e l'*interferenza illecita* rispetto agli stessi (art. 4).

La direttiva 2016/1148 (c.d. direttiva NIS) predispone un articolato sistema di prevenzione dei *rischi* e degli *incidenti* che possono interessare le reti ed i sistemi di informazione – ai quali viene riconosciuto un ruolo vitale nella società - prescindendo dall'introduzione di nuove fattispecie criminose e prescrivendo agli Stati l'adozione di misure, che, sotto il profilo formale, hanno natura amministrativa. La «*sicurezza della rete e dei sistemi informativi*» è definita come la capacità di resistere ad ogni azione che possa compromettere la *disponibilità*, l'*autenticità*, l'*integrità* o la *riservatezza* dei dati conservati, trasmessi o trattati attraverso le reti o i sistemi informativi (art. 4, par. 2). La direttiva promuove l'attiva collaborazione e lo scambio di informazioni fra i soggetti a vario titolo coinvolti nell'uso del *cyberspace*, con l'istituzione di apposite strutture, quali, ad esempio, il «punto di contatto unico nazionale» (art. 8) e il CISRT (art. 9).

Il regolamento 2019/881 (c.d. *Cybersecurity Act*) attribuisce all'*Agenzia per la cybersecurity* (ENISA) il compito di attuare la strategia di prevenzione dei *cybercrimes* e del cyberterrorismo, assistendo gli Stati nell'elaborazione di *piani strategici nazionali* per rilevare e analizzare le minacce e gli incidenti cibernetici (art. 6) e perseguendo un elevato livello di «*cyberresilienza*» (art. 1, par. 1). Questa consiste in un processo adattivo legato ad un cambiamento di contesto o di sistema, secondo una prospettiva proattiva, volto a rilevare le minacce cibernetiche contro le infrastrutture critiche dello Stato ed intervenire tempestivamente con misure atte a scongiurare l'interruzione delle funzioni vitali dello Stato.

Il diritto eurounitario si è occupato anche dell'interazione fra cibernetica e terrorismo (pur senza mai impiegare il termine cyberterrorismo, a differenza della legislazione di settore statunitense), adottando un *approccio multilivello* per la

prevenzione del fenomeno, che prevede sia fattispecie di reato sia misure di prevenzione.

La direttiva 2017/541 sulla lotta contro il terrorismo, che ha sostituito la decisione-quadro 2002/475/GAI, impone l'adozione di fattispecie criminose che vengono tipizzate alquanto dettagliatamente (a dispetto del limite delle norme minime fissato dell'art. 83 TFUE) e presentano profili di incompatibilità con i principi costituzionali che orientano il diritto penale italiano. A titolo esemplificativo giova osservare che la *pubblica provocazione per commettere reati di terrorismo* (art. 5 della direttiva) può astrattamente integrarsi nel caso della pubblicazione di *posts* o commenti che, sebbene affini ad ideologie contrarie a quelle della maggioranza politica o connotati da toni estremistici, non siano oggettivamente idonei ad istigare alla commissione di un reato terroristico, la cui realizzazione - atteso l'elemento psicologico del dolo specifico - non è necessaria. La direttiva prescrive altresì l'adozione di *misure predelittuali* per scongiurare la commissione dei reati di terrorismo. Tra queste figura la *rimozione dei contenuti online* che possono provocare la commissione di reati di terrorismo (art. 21, par. 1), con la precisazione che, nel caso di inapplicabilità della misura, gli Stati devono *bloccare l'accesso* agli stessi (art. 21, par. 2).

Il regolamento 2021/784, invece, prevede che gli Stati adottino strumenti volti a contrastare la diffusione *online* di contenuti con finalità terroristiche e l'utilizzo dei servizi di *hosting* per i medesimi scopi. Attraverso gli «*ordini di rimozione*» (art. 3) l'Autorità competente - ricorrendo *casi di emergenza debitamente giustificati* - impone (senza preavviso) ai prestatori di servizi di *hosting* la *rimozione* dei contenuti *online* o la *disabilitazione* dell'accesso agli stessi in tutti gli Stati membri (art. 3, par. 1). Il regolamento prescrive che il carattere terroristico dei contenuti debba valutarsi in base alla «*natura*», al «*contesto*», alla «*formulazione*» e al «*potenziale* di portare a conseguenze dannose, compromettendo la sicurezza e l'incolumità delle persone» della pubblicazione (Considerando 11). Tra le misure specificamente dedicate alla prevenzione della radicalizzazione terroristica il regolamento prevede lo sviluppo dell'«*alfabetizzazione mediatica*», del «*pensiero critico*», delle «*narrazioni*

alternative», delle «*controargomentazioni*» e del «*dialogo con le comunità interessate*» (Considerando 2).

L'esame delle fonti europee in materia di terrorismo *online* conferma come in ambito sovranazionale si sia adottato un *approccio multisettoriale* e *multilivello* per prevenire il fenomeno, combinando tra loro «misure legislative», «misure non legislative» e «misure volontarie» (anche non penali), basate sulla collaborazione di soggetti pubblici e privati (Considerando 3).

L'ordinamento italiano non disciplina in via autonoma il cyberterrorismo e l'unica disposizione direttamente rilevante in materia è l'art. 270-*quinquies*, co. 2, c.p., ove si prevede un aumento di pena per le condotte di addestramento ad attività con finalità di terrorismo realizzate con strumenti informatici o telematici. In effetti il legislatore italiano, adottando l'impostazione *tool oriented*, ha ritenuto che il cyberterrorismo sia null'altro che una delle possibili forme di manifestazione delle condotte del terrorismo comune, come tale sussumibile nelle fattispecie previste dagli artt. 270-*bis* e ss. c.p. Queste, come si è detto, vengono impiegate per perseguire precipuamente aspirazioni prevenzionistiche - speciali e generali - attraverso tecniche di incriminazione che, combinando la *struttura dei reati di pericolo* con l'elemento psicologico del *dolo specifico*, estendono la soglia della punibilità in senso anticipatorio, anche oltre il tentativo punibile. In ogni caso il sistema delle fattispecie previste nel Capo I del Titolo I del Libro II del codice penale è inadeguato a soddisfare le istanze di prevenzione contro il cyberterrorismo avanzate dal diritto europeo, perché non tiene conto delle peculiarità del *cyberspace* e presenta profili di criticità rispetto ai principi del diritto penale costituzionalmente orientato. Come osserva autorevole dottrina, la dilatazione a fini prevenzionistici della pena – che per natura deve essere irrogata *post delictum* all'esito di un processo che accerti la responsabilità dell'imputato - comporta una caduta di livello della serietà e dell'efficacia del sistema penale, perché strumentalizza ingiustamente e banalizza al contempo il rimprovero, rendendosi dunque opportuno ricercare degli strumenti alternativi.

Le misure di prevenzione italiane, oggi disciplinate dal d.lgs. 159/2011 (c.d. *Codice delle leggi antimafia e delle misure di prevenzione*, che ha abrogato

la l. 1423/1956), sono strumenti formalmente amministrativi ma sostanzialmente penali che intervengono sulla libertà personale (*rimpatrio con foglio di via obbligatorio*, *avviso orale*, *sorveglianza speciale di pubblica sicurezza*) o sul patrimonio (principalmente *confisca* e *sequestro*) *ante delictum* in funzione special-preventiva. Esse, infatti, producono effetti limitatavi della libertà personale, che possono essere equivalenti a quelli della pena (pur non rispondendo ad una logica sanzionatoria). Autorevole dottrina ha criticato le misure di prevenzione, avanzando dubbi circa la loro compatibilità con il sistema dei principi costituzionali.

L'applicazione delle misure di prevenzione postula particolari presupposti di natura soggettiva ed oggettiva. Sotto il primo profilo, il prevenuto deve appartenere ad una delle categorie previste dall'art. 4 del Codice Antimafia (che individuano i reati che possono essere prevenuti, tra i quali figurano l'*associazione di tipo mafioso* ed il *terrorismo*). Tra i presupposti di carattere soggettivo, invece, figura la *pericolosità sociale del prevenuto*, che - diversamente dalla definizione prevista dall'art. 203 c.p. - consiste nella *probabilità* che il proposto commetta futuri reati. La sussistenza, concreta ed attuale, della pericolosità sociale deve essere valutata sulla base di un apposito giudizio articolato in una prima fase *cognitiva* e in una seconda *prognostica*, avvalendosi di criteri oggettivi (da impiegare unitamente a quelli dettati dell'art. 133, co. 2, c.p.) che il legislatore, tuttavia, non ha individuato. Per quanto attiene ai requisiti applicativi di tipo oggettivo, invece, essi si ricavano dalle stesse categorie previste dall'art. 4 del d.lgs. 159/2011. Più precisamente la lettera d) della disposizione da ultimo richiamata postula la sussistenza di indizi in relazione ad un reato di terrorismo o il compimento di «*atti preparatori obiettivamente rilevanti*» ovvero «*esecutivi diretti*» alla commissione di reati con finalità di terrorismo. La dottrina ha condivisibilmente criticato la previsione in parola, osservando che consentirebbe di applicare le misure di prevenzione - che possono produrre effetti limitativi della libertà personale equivalenti a quelli della pena - ad atti preparatori sguarniti dei requisiti garantistici richiesti per la punibilità del tentativo di delitto, soglia minima della rilevanza penale. Orbene, se, da un lato, è vero che le misure

di prevenzione - per loro stessa definizione - devono intervenire prima della commissione del reato (o del suo tentativo), dall'altro lato, è indispensabile che siffatte misure afflittive vengano irrogate sulla base di determinati requisiti oggettivi che, sebbene non coincidenti con quelli previsti dall'art. 56 c.p. (che renderebbero applicabile la pena), abbiano comunque l'effetto di garantire l'inviolabilità della libertà personale, eccezionalmente limitabile alle condizioni dell'art. 13 Cost.

La giurisprudenza europea e nazionale si è occupata in tempi relativamente recenti delle misure di prevenzione, inaugurando un *dialogo "mediato"* fra Corti.

La Grande Camera della Corte Europea dei Diritti dell'Uomo, con la sentenza 23.2.2017, De Tommaso c. Italia (ricorso n. 43395/09), ha statuito che gli artt. 1, 3 e 5 della l. 1423/1956 – e, quindi, gli artt. 1, 6 e 8 d.lgs. 159/2011 che ne riproducono oggi il contenuto - contrastano con la libertà di circolazione (art. 2 del Protocollo addizionale IV alla CEDU). In particolare le disposizioni nazionali sono prive del requisito della *prevedibilità* – con violazione dei principi della certezza del diritto e della determinatezza – che, unitamente all'*accessibilità* e alla *base legale*, deve connotare le misure volte alla limitazione della suddetta libertà. La Corte di Strasburgo, pur non attribuendo natura formalmente penale alle misure di prevenzione, ha ritenuto che - attesa la limitazione della libertà personale che possono produrre – esse debbano soggiacere al principio di legalità ed ai suoi corollari di determinatezza e tassatività.

La Corte Costituzionale, con sentenza 24.1.2019, n. 24, ha dichiarato l'illegittimità costituzionale dell'art. 1, lett. a), d.lgs. 159/2011 (già art. 1, n. 1, l. 1423/1956), censurandone l'indeterminatezza rispetto all'art. 13 della Costituzione. I giudici di legittimità hanno preliminarmente osservato che, in via generale, la *ratio* delle misure di prevenzione non è incompatibile con i principi costituzionali. Tuttavia, attesa l'afflittività degli strumenti in parola, essi devono essere assoggettati ad un complesso di garanzie che, in accordo all'interpretazione dei giudici italiani, sono più stringenti rispetto a quelle individuate dalla Corte europea. Più precisamente, secondo la Corte Costituzionale, oltre al *principio di legalità* ed ai suoi corollari della *riserva di legge* (base legale) e della

determinatezza (prevedibilità), le misure di prevenzione devono rispettare la *proporzionalità* fra il grado di afflittività della misura e la gravità del reato che si intende prevenire ed essere soggette alla *riserva di giurisdizione*. In altri termini si è ritenuto che, pur senza riconoscere natura formalmente penale alle misure di prevenzione, queste debbano rispettare gli stessi principi che orientano il diritto penale costituzionale.

Nella seconda parte della sentenza, la Corte si è interrogata circa la possibilità di rendere costituzionalmente conformi le disposizioni sottoposte al suo vaglio - peculiarmente sotto il profilo della determinatezza e, quindi, della prevedibilità - e sullo strumento da impiegare a tal fine. Secondo i giudici, le disposizioni in parola possono essere ricondotte entro il perimetro della costituzionalità, attraverso una *lettura tassativizzante costituzionalmente orientata*. Questa deve prevedere la determinazione delle caratteristiche dei reati (e non i singoli titoli) che si possono prevenire, i quali – nel caso delle misure di prevenzione patrimoniali delle quali i giudici, nella sentenza, si occupano più nel dettaglio - presuppongo che: a) gli atti siano abituali; b) detti atti abbiano prodotto profitti in capo al proposto; c) il profitto abbia costituito - in una determinata epoca – l'unico reddito del soggetto (o quantomeno una componente significativa dello stesso). Tuttavia il correttivo ermeneutico può operare solo in relazione alle norme che presentano un grado di imprecisione *lieve*, quale è l'art. 1, lett. b) del d.lgs. 159/2011, di cui la Corte ha quindi ritenuto la legittimità costituzionale.

La giurisprudenza sovranazionale e quella domestica sembrano concordi nel ritenere che la disciplina delle misure di prevenzione, attesa la loro afflittività, debba essere ricondotta entro l'alveo della *matière pénale*, quantomeno sotto il profilo sostanziale, con l'applicazione delle relative garanzie.

L'esigenza di determinatezza e prevedibilità si fa ancor più forte in un settore, come quello del cyberterrorismo, contraddistinto dal *cyberspace*, le cui caratteristiche rendono difficile se non impossibile l'inquadramento del fenomeno entro le categorie tradizionali del diritto penale.

Nel caso del terrorismo cibernetico si dovrebbe dunque procedere - *de iure condendo* - all'integrazione del disposto dell'art. 4 del d.lgs. 159/2011 attraverso

un'apposita categoria soggettiva dedicata al fenomeno, in cui sia il legislatore a tassativizzare gli *indizi*, gli «*atti preparatori obiettivamente rilevanti*» e gli «*atti esecutivi diretti*» alla commissione del reato, tali da giustificare l'applicazione delle misure di prevenzione. Solo in questo modo i consociati potranno prevedere, con sufficiente precisione, se i comportamenti che hanno posto in essere possano comportare la limitazione della loro libertà personale in fase predelittuale.

In proposito si potrebbe elaborare il concetto di *pericolosità sociale cibernetica*, per la cui valutazione, oltre agli indici già previsti dall'art. 4, lett. d) del Codice Antimafia - si dovrà tener conto dei seguenti criteri: a) il *modo che il proposto adotta per comunicare nel cyberspace*, con particolare attenzione per il *contenuto* delle pubblicazioni e per i loro *destinatari*; b) il *modo di relazionarsi virtualmente con gli altri utenti*; c) le *reazioni del soggetto alle pubblicazioni altrui*.

Ad ogni buon conto l'inadeguatezza dell'attuale sistema delle misure di prevenzione rispetto al cyberterrorismo emerge anche in relazione ai singoli strumenti tradizionalmente impiegati nel nostro ordinamento, che possono essere applicati solo laddove sia individuato il prevenuto o il suo patrimonio, circostanza che nel *cyberspace* non è facilmente realizzabile. Il diritto eurounitario ed alcuni settori normati da leggi speciali offrono degli spunti per elaborare misure di prevenzione efficaci contro il terrorismo cibernetico.

Per quanto riguarda il diritto europeo si sono già ricordate le misure della *rimozione* e del *blocco* (previste dalla direttiva 2017/541) e degli *ordini di rimozione* e della *disabilitazione* (previste dal regolamento 2021/784).

In ambito militare, invece, vengono da tempo impiegati dei modelli operativi che, adattandosi alla dinamica dell'attacco, sono volti a gestirne ogni fase (pre-attacco, attacco e post-attacco) per minimizzare gli effetti negativi che possono derivarne alla struttura presa di mira. La fase di pre-attacco prevede una prima fase cognitiva - volta a reperire informazioni su potenziali attacchi cibernetici - e una seconda fase volta ad elaborare strategie per impedire l'attacco o, quantomeno, intervenire sulla struttura con misure che lo rendano inefficace.

L'art. 7 del d.lgs. 231/2001, recante norme in materia di responsabilità da reato delle persone giuridiche, prevede che gli enti adottino un *modello di gestione e controllo* per la prevenzione dei reati presupposto previsti dal successivo art. 24 (fra questi figurano i reati informatici e i reati di terrorismo). Ebbene si ritiene che la disciplina prevista dal d.lgs. 231/2001 debba essere aggiornata, includendo i *cybercrimes* e il cyberterrorismo tra i reati presupposto e consentendo l'applicazione del *modello* agli enti pubblici e in particolare alle infrastrutture critiche cibernetiche dello Stato.

Più di recente, con la legge 29.5.2017, n. 71, è stata normata *extra codicem* la prevenzione del *cyberbullismo*, materia interessata da talune delle criticità emerse in relazione al cyberterrorismo. Infatti il fenomeno è considerato un fatto penalmente rilevante - come emerge dalla definizione di cui all'art. 1, co. 2, l. 71/2017 - ancorché ne manchi la tipizzazione in un'apposita fattispecie autonoma. L'approccio preventivo adottato in questa materia prevede una *strategia di attenzione*, *tutela* ed *educazione* nei confronti dei minori (art. 1, co. 1, l. 71/2017), l'istituzione di appositi organismi per monitore e studiare il fenomeno (tra i quali un «tavolo tecnico per la prevenzione e il contrasto del cyberbullismo»), un «piano di azione integrato per il contrasto e la prevenzione del cyberbullismo» che coinvolga i fornitori dei servizi di *social networking* (art. 3, par. 3) e la promozione di un processo di *alfabetizzazione cibernetica* (art. 4, co. 5, l. 71/2017).

In via principale la l. 71/2017 prevede l'adozione di misure di *positive prevention*. Trattasi di strumenti predelittuali che, anziché limitare la libertà del proposto, ne incrementano la sfera giuridica personale e ne promuovono il benessere individuale (con iniziative di tipo prettamente sociale, politico e culturale), al fine di evitare che si determini a commettere reati in futuro. Trattasi di una novità per l'ordinamento italiano, atteso il tradizionale impiego in via esclusiva di *misure di prevenzione negativa* (previste dal d.lgs. 159/2011), che comunque la l. 71/2017 prevede. Invero contro il bullismo cibernetico è ammesso il ricorso all'*ammonimento* (art. 7) ed alle misure dell'*oscuramento*, della

rimozione e del *blocco* (art. 2), queste ultime impiegate per evitare la reiterazione del reato.

Alla luce delle analogie sussistenti fra *cyberbullismo* e *cyberterrorismo* pare dunque opportuno integrare il sistema delle misure di prevenzione contro il secondo con strumenti di *positive prevention* (*sociale* e *situazionale*), i quali intervengano sugli elementi della *natura*, del *contesto* e della *pericolosità sociale cibernetica*, azzerando l'obiettiva rilevanza degli atti preparatori rispetto alla commissione del reato.

Orbene, l'ordinamento italiano, con la legge sul cyberbullismo, ha inaugurato una nuova tecnica di prevenzione dei *cybercrimes*, maggiormente rispondente alle previsioni europee in materia, applicabile anche al cyberterrorismo. Essa, discostandosi dall'impostazione tradizionale, contrappone alla scriteriata iperproduzione di fattispecie di reato prevenzionistiche un sistema integrato di misure di prevenzione negative e positive, con preferenza per le seconde. Detto approccio multilivello, oltre a soddisfare le istanze europee in materia, consente di intervenire *ante delictum* in funzione specialpreventiva con maggior flessibilità, salva la necessità di tassativizzare categorie di prevenuti connotate, sotto il profilo oggettivo, da sufficiente prevedibilità e determinatezza, anche in punto di *pericolosità sociale cibernetica*.

BIBLIOGRAFIA

ACCINNI G. P., *Cybersecurity e criptovalute. Profili di rilevanza penale dopo la Quinta Direttiva*, in *Sist. Pen*., 5/2020, p. 211.

ALLEGRIA A., *Diritto d'accesso, diritti e doveri nell'uso di internet*, in ALLEGRIA A., DI STEFANO M., FEDERICI F. (a cura di), *Il diritto del web. Rete, Intelligence e Nuove Tecnologie*, Primiceri, 2017, p. 160.

BALBO P., *Il terrorismo le fattispecie di un reato in evoluzione nelle disposizioni italiane ed internazionali*, Halley, 2007.

BALSAMO A., *Diritto dell'UE e della CEDU e confisca di prevenzione*, in *Il Libro dell'anno del diritto*, Istituto della Enciclopedia Italiana, 2014.

BALSAMO A., *Decreto Antiterrorismo e riforma del sistema delle misure di prevenzione*, in *Dir. Pen. Cont.*, 3/2015, p. 10.

BALSAMO A., D'AGOSTINO V., *Inquadramento sistematico ed evoluzione storica delle misure di prevenzione patrimoniali*, in AA.VV., F. FIORENTIN (a cura di), *Le misure di prevenzione personali e patrimoniali*, Giappichelli, 2018, p. 501.

BARAVELLI A., *Per una storia della risposta penale al terrorismo italiano (1976-82),* Meridiana, 2020.

BARTOLI R., *Lotta al terrorismo internazionale. Tra diritto penale del nemico, jus in bello criminale e annientamento del nemico assoluto*, Giappichelli, 2008.

BARTOLI R., *L'accesso abusivo a un sistema informatico (art. 615-ter c.p.) a un bivio ermeneutico teleologicamente orientato*, in *Dir. Pen. Cont*., 1/2012, p. 123.

BARTOLI R., PELISSERO M., SEMINARA S., *Diritto penale – Lineamenti di parte speciale*, Giappichelli, 2021.

M. BARTOLOMÉ, *Cybersecurity in the second decade of the Twenty-First Century*, in AA.VV., J. CAYÓN PEÑA (a cura di), *Security and defence: ethical and legal challenges in the face of current conflicts*, Springer, 2022.

BASILE F., *Dieci anni di codice antimafia – le misure di prevenzione: bilanci e prospettive*, in *Rivista di Studi e Ricerche sulla criminalità organizzata*, 3/2021, p. 16.

BATTAGLINI C., *Le misure patrimoniali antiterrorismo alla prova dei principi dello stato di diritto*, in *Dir. Pen. Cont.*, 1/2017, p. 59.

BELLACOSA M., *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle sezioni* unite, in *Dir. Pen. Comp.*, 2.2.2015, p. 2.

BELLO B. G., SCUDIERI L., *L'odio online: forme, prevenzione e contrasto*, Giappichelli, 2022.

BENDONI M., *Assalto al cantiere T.a.v. di Chiomonte: non fu terrorismo*, in *Cass. pen*., 6/ 2015, p. 2266.

BENIGER J. R., *The Control Revolution: Technological and Economic Origins of the Information Society*, Harvard University Press, 1986.

BENUSSI C., BRUNELLI D., *Il reato portato a conseguenze ulteriori, problemi di qualificazione giuridica*, Giappichelli, 2000.

BERARDI A., *Le pene principali*, in M. RONCO (a cura di), *Persone e sanzioni. Presupposti soggettivi, previsione, comminazione ed esecuzione delle sanzioni penali*, Zanichelli, 2010.

BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 9/1995, p. 2333.

BHARDWAJ A., SAPRA V., *Security Incidents & Response Against Cyber Attacks*, Springer International Publishing, 2021.

BIANCHI A., *Manuale delle società di capitali*, CEDAM, 2012.

BIN R., PITRUZZELLA G., *Diritto Costituzionale*, Giappichelli, 2021.

BOBBIO N., voce «*Sanzione*», in *Nov. Dig. It.*, XVI, UTET, 1969, p. 531.

BODEAU D. J., GRAUBART R. D., MCQUAID R., PILLITTER V., ROSS R., *Developing Cyber Resilient Systems. A Systems Security Engineering Approach*, vol. 2, Draft NIST Special Publication, 2019.

BODEAU D. J., GRAUBART R. D., MCQUAID R. M., WOODILL J., *Cyber Resiliency Metrics Catalog*, Mitre, 2018.

BONFANTI A., *Attacchi cibernetici e cyber war: considerazioni di diritto internazionale*, in *Notizie di Politeia*, vol. 132, 2018, p. 118.

BONTEMPI V., *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, Roma TrE-Press, 2022.

BORGOBELLO M., *La Cassazione sul rapporto tra accesso abusivo a sistema informatico, frode informatica e detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*, in *Giur. Pen. web,* 1/2020.

BORRUSO R., *La tutela del documento e dei dati*, in BORRUSO R., BUONOMO G., CORASANITI G., D'AIETTI G. (a cura di), *Profili penali dell'informatica*, Giuffrè, 1994.

BRANDEIS L. D., WARREN S. D., *The Right To Privacy*, in *Harv. Law Rev.*, 5/1890, p. 193.

BRANTINGHAM P. L., BRANTINGHAM P. J., TAYLOR W., *Situational Crime Prevention as a Key Component in Embedded Crime Prevention*, in *Canadian J. Criminology & Crim. Just*., 47, 2005, p. 276.

BRIGHI R., CHIARA P. G., *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi*, 21/2021, p. 18.

BRIZZI F., PALAZZO P., PERDUCA A., *Le nuove misure di prevenzione personali e patrimoniali*, Maggioli, 2012.

BRIZZI F., *Il terrorismo internazionale*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali*, Giappichelli, 2018, p. 465.

BRUNO L. G., *Misure di prevenzione patrimoniali e congelamento dei beni per reati di terrorismo: problemi sostanziali e processuali*, in *Dir. Pen. Proc.*, 2007, p. 99.

BUCHAN R., TSAGOURIAS N., *International Law and Cyber Space*, Cheltenham, 2015.

BUONO L., *The Global Challenge of Cloud Computing and EU Law*, in *Eucrim*, 3/2010, p. 117.

CADOPPI A., VENEZIANI P., *Elementi di diritto penale – Parte generale,* CEDAM, 2021.

CAMPAGNOLI M. N., *Informazione, social network & diritto*, Key Editore, 2020.

CANEPARI L., la voce "*Computer*", in *Il DiPI – Dizionario di pronuncia italiana*, Zanichelli, 2009.

CARRINO A., *Kelsen e il problema della Sovranità*, Ed. Sc. It., 1990.

CARTABIA M., *La convenzione europea dei diritti dell'uomo e l'ordinamento italiano*, in BALSAMO A., KOSTORIS R. E. (a cura di), *Giurisprudenza europea e processo penale italiano*, Giappichelli, 2008.

CARTWRIGHT J. E., *Memorandum for chiefs of the military services commanders of the combatant commands directors of the joint staff directorates*, on *Joint Terminology for Cyberspace Operations*, USDOD, 2011.

CASALE P., *Prima "legge" della sicurezza informatica: "un computer sicuro è un computer spento"*, in *Arch. Pen.*, 2/2021, p. 8.

CASTIGLIONI L., MARIOTTI S., *IL - Vocabolario della lingua latina*, Loescher, 1979, sub *terrĕo, ĕs, terrŭi, terrĭtum, ēre*, p. 1466.

CAVALLA F., *Retorica giudiziale, logica e verità*, in *Retorica, processo, verità*, Franco Angeli, 2007.

CENTONZE S., GIOVEDI L., *Terrorismo e legislazione d'emergenza*, Key, 2016.

CERQUA L. D., *La nozione di terrorismo tra diritto interno, diritto internazionale e diritto comunitario*, in MANES V. (a cura di), *L'interpretazione conforme al diritto comunitario in materia penale*, Bononia University Press, 2007, p.120.

CERUZZI P. E., *Storia dell'informatica. Dai primi computer digitali all'era di Internet*, Apogeo, 2006.

CERVI M., MONTANELLI I., *L'Italia degli anni di piombo* (1965-1978), in MONTANELLI I. (a cura di), *Storia d'Italia*, Vol. XIX, BUR, 2022.

CHIARAMONTE X., SENALDI A., *Violenza politica*, Ledizioni, 2018.

CIPOLLA P., sub *Art. 615-ter c.p.*, in AA.VV., LATTANZI G. (a cura di), *Codice penale annotato con la giurisprudenza*, Giuffrè, 2020, p. 1993.

CIVELLO CONIGLIARO S., *La nuova tutela penale europea dei sistemi di informazione*, in *Dir. Pen. Comp*., 30.10.2013, p. 5.

CLARK D., *Characterizing Cyberspace: Past, Present, and Future*, in *MIT Review*, 3/2010, p. 10.

CLARKE R.V., *Situational Crime Prevention*, in *Crime & Just*., 19/1995, p. 91.

COCCO G., *Beni giuridici funzionali versus bene giuridico personalistico*, in AA.VV. *Studi in onore di Giorgio Marinucci*, vol. I, *Teoria del diritto penale criminologia e politica criminale*, Giuffrè, 2006, p. 179.

COCCO G., *Il fatto tipico. Questioni della postmodernità. Tra reati di mero comportamento e tutela di beni funzionali*, in COCCO G., AMBROSETTI E. M. (a cura di), *Trattato breve di diritto penale - Parte generale*, Vol. I, 2021, p. 59.

COCCO G., AMBROSETTI E. M., *Trattato breve di Diritto Penale - Parte generale*, CEDAM, 2021.

COCCO G., AMBROSETTI E. M., *Trattato breve di Diritto Penale - Parte speciale*, CEDAM, 2021.

COHEN D., *L'evoluzione del terrorismo contemporaneo nel cyber-spazio*, in *Gnosis*, 2/2016, p. 118.

COLAIOCCO S., *Le nuove norme antiterrorismo e le libertà della persona: quale equilibrio?*, in *Arch. pen*., 2/2015, p. 5.

COLAPAOLI F., COPPOLA A., GRAZIANI M. R., MIRONI M., *I social network*, in AA.VV., *Social network e diritto*, Giappichelli, 2021.

CONCETTI C., *Cybersecurity: Unione europea e Italia. Prospettive a confronto*, Nuova cultura, 2014.

CHOOBCHIAN P., ROZENBERG J., ZOU B., *Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies*, JTS, 2021.

COMMISSIONE EUROPEA, *Proposta di direttiva sulla resilienza dei soggetti critici* COM(2020) 829 final., disponibile al *link*: *https : / / eur – lex . europa . eu /legal – content / IT / TXT / PDF / ?uri = CELEX : 52020PC0829&from = IT*.

CORRADINI I., *Building a Cybersecurity Culture in Organizations*, Springer International Publishing, 2020.

CORTESI M. F., FILIPPI L., *Il Codice delle misure di prevenzione*, Giappichelli, 2011.

CORTESI M. F., *Le "nuove" misure di prevenzione personali*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali,* Giappichelli, 2018, p. 215.

COSTA D., *La responsabilità dell'Internet Service Provider per i reati in materia di diritto* d'autore, in *Giur. Pen*., 2/2022, p. 47.

CRESTI S., *L'elasticità di resilienza*, Accademia della Crusca, 12.12.2014, in *https://accademiadellacrusca.it/it/consulenza/lelasticit%C3%A0-diresilienza/928*.

CRISPINO S., *Finalità di terrorismo, snodi ermeneutici e ruolo dell'interpretazione conforme. I giudici tra indeterminatezza delle fattispecie e fonti sovranazionali*, in *Dir. Pen. Cont*., 1/2017, p. 227.

CRISTALLINI A., RAZZANTE R., *Cybercrime tra diritto ed economia*, Pacini, 2021.

CUPELLI C., *Il nuovo art. 270-bis c.p.: emergenze di tutela e deficit di determinatezza?*, in *Cass. pen.*, 2/2002, p. 901.

DARNIS J. P., POLITO C., *La Geopolitica del digitale*, Nuova cultura, 2019.

DELLA RAGIONE L., *Le misure di prevenzione nello specchio del volto costituzionale del sistema penale*, in *Discrimen*, 20.4.2020.

DELLA TORRE L., *Tra guerra e terrorismo: le giurisprudenze nazionali alla prova dei foreign fighters*, in *Dir. Pen. Comp*., 2/2017, p. 170.

DENNING D. E., *Cyberterrorism*, Georgetown University, 2000.

DENNING E. D., *Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, in ARQUILLA J., RONFELDT D., *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defence Research Institute RAND, 2001.

DE VIVO M. C., RICCI G., *Diritto, crimini e tecnologie*, in *Informatica e diritto*, 2/2012, p. 14.

DE ZAYAS A.*, Human rights and indefinite detention*, in *International review of the red cross*, 87/2005, p. 6.

DOMENICALI C., *Tutela della persona negli spazi virtuali: la strada del "domicilio informatico"*, in *Federalismi*, 28.3.2018, p. 8.

D'ONOFRIO C., *Il cyberbullismo*, in CORONA F. (a cura di), *Reati informatici e investigazioni digitali. Diffamazione via web – Prove digitali – Sex crimes – Cyberstalking – Cyberbullismo – Reati privacy*, Pacini Giuridica, p. 169.

DURANTE M., PAGALLO U., *Manuale di informatica giuridica e diritto delle nuove tecnologie*, UTET, 2012.

EDWARDS L., HARINJA E., SCHAFER B., *Future Law, Emerging technology, regulation and ethics*, Edinburgh University Press, 2020.

EVEN S., SIMAN-TOV D., *Cyber Warfare: Concepts and Strategic Trends*, Memorandum 117, The Institute for National Security Studies, 2012.

FARRINGTON D.P., TONRY M., *Building a Safer Society*, *Strategy Approaches to Crime Prevention*, University of Chicago Press, 1995.

FARRINGTON D. P., MACKENZIE D. L., SHERMAN L. W., WELSH B. C., *Evidence-based Crime prevention*, Routledge, 2002.

FARRINGTON D. P., WELSH B. C., *The Oxford Handbook of Crime Prevention*, Oxford University Press, 2014.

FATTORE M., *Così lontani così vicini: il diritto penale e le misure di prevenzione Osservazioni su Corte EDU, Grande Camera, 23 febbraio 2017, De Tommaso c. Italia*, in *Dir. Pen. Cont*., 4/2017, p. 97.

FERRARESE M. R., *Diritto sconfinato. Inventiva giuridica e spazi nel mondo globale*, Laterza, 2007.

FIANDACA G., MUSCO E., *Diritto penale – Parte generale*, Zanichelli, 2021.

FILEDS Z., PATRICK H., VAN NIKERK B., *Cyber Law, Privacy, and Security*, IGI Global, 2019.

FIORENTIN F. (a cura di), *Misure di prevenzione personali e patrimoniali*, Giappichelli, 2018.

FLEMING P., STOHL M., *Myths and Realities of Cyberterrorism*, *in* l'*International Conference on Countering Terrorism Through Enhanced International Cooperation*, 22.9.2000, p. 30.

FLOR R., *Phishing, identity theft, e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. It. dir. e proc. pen.*, 2007, p. 899.

FLOR R., *Art. 615-ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. Pen. Proc.*, 1/2008, p. 134.

FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. trim. dir. pen. ec.*, 3/2009, p. 705.

FLOR R., *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *Dir. Pen. Comp*., 20.9.2012, p. 2.

FLOR R., *Verso una rivalutazione dell'art. 615 ter c.p.?*, in *Dir. Pen. Cont.*, 2/2012, p. 126.

FLOR R., *Cyber-terrorismo e diritto penale in Italia*, in WENIN R., FORNASARI G. (a cura di)*, Diritto penale e modernità. Le nuove sfide fra terrorismo*, *sviluppo tecnologico e garanzie fondamentali*, ed. Università degli Studi di Trento, 2017, p. 357.

FLOR R., *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in AA.VV., CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrimes. Diritto e procedura penale dell'informatica*, UTET, 2019, p. 150.

FLOR R., *Cyber-criminality*: *le fonti europee ed internazionali*, in AA.VV., CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrimes. Diritto e procedura penale dell'informatica*, UTET, 2019, p. 125.

FRAGOLA S. P., *Le misure di prevenzione*, CEDAM, 1992.

FRANKOWSKI S., SHELTON D., *Preventive Detention. A Comparative and International perspective*, Martinus Nijhoff, 2022.

FURFARO S., *In tema di superamento delle presunzioni nel giudizio di prevenzione*, in *Giur. It*., 7/2013, p. 1655.

GALLO E., MUSCO E., *Delitti contro l'ordine costituzionale*, Patron, 1984.

GAROFOLI R., *Il contrasto ai reati di impresa nel d.lgs. n. 231 del 2001 e nel d.l. n. 90 del 2014: non solo repressione, ma prevenzione e continuità aziendale*, in *Dir. Pen. Cont*., 30.9.2015, p. 2.

GAROFOLI R., *Manuale di diritto penale - Parte speciale*, Neldiritto, 2022.

GAYREL C., GÉRARD J., MOINY J. P., POULLET Y., VAN GYSEGHEM J. M., *Cloud computing and its implications on data protection, Discussion paper*, Council of Europe, Strasbourg, 2010.

GIBSON W., *Neuromancer*, Berkley Publishing, 1989.

GIBSON W., *Burning Chrome*, Harper Collins, 2003.

GIORDANA N., *L'art. 270-bis disciplina cardine dell'antiterrorismo. Un vestito sempre attuale che si conforme alle recenti correnti fondamentaliste di matrice islamica*, in *Giur. Pen. web*, 20.12.2014.

GIUDICI A., *Tentativo e atti preparatori: una questione sempre aperta*, in *Dir. Pen. Cont*., 1.6.2012, p. 4.

GORI U., LISI S., *Information warfare 2012. Armi cibernetiche e processo decisionale*, Franco Angeli.

GORI U., LISI S., *Cyber Warfare. Armi cibernetiche, sicurezza nazionale e difesa del buesiness*, Franco Angeli, 2014.

GORI U., *Lo spazio cibernetico e la sicurezza nazionale. Le nuove minacce cyber*, in *Lo spazio cibernetico tra esigenze di sicurezza nazionale e tutela delle libertà individuali*, supplemento al n. 6/2014 di *Informazioni della Difesa*, p. 8.

DE GRAAF J., SCHMID A. P., *Violence as communication: Insurgent terrorism and the western news media*, SAGE Publications, 1982.

GRANDI C., *Le conseguenze penalistiche delle condotte di cyberbullismo. Un'analisi de jure condito*, in *Annali online della Didattica e della Formazione Docente*, Vol. 9, 13/2017, p. 40.

GRANT H., *Social Crime Prevention in the Developing World Exploring the Role of Police in Crime Prevention*, Springer, 2014.

GRASSO G., *Le misure di prevenzione personali e patrimoniali nel sistema costituzionale*, in *Sist. Pen.*, 14.2.2020, contributo disponibile al link: *https://www.sistemapenale.it/pdf_contenuti/1581636989_grasso-2020a-misure-prevenzione-sistema-costituzionale.pdf.*

GROSSO C. F., *Su di un'interessante controversia interpretativa in tema di luogo del commesso reato e di giudice competente per territorio in materia di accesso abusivo in un sistema informatico*, in *Riv. it. dir. proc. pen.*, 2014, p. 1704.

GUERRINI R., MAZZA L., RIONDATO S., *Le misure di prevenzione. Profili sostanziali e processuali*, CEDAM, 2004.

GUPTA B., SRINIVASAGOPALAN S., *Handbook of Research on Intrusion Detection Systems*, IGI Global, 2020.

HAUSKEN K., *Cyber resilience in firms, organizations and societies*, in *Internet of things*, 11/2020, p. 2.

HENDERSHOT H. M., *CyberCrime 2003 – Terrorists' Activity in Cyberspace*, *briefing slides from the Cyber Division*, *Briefing slides from the Cyber Division, Federal Bureau of Investigation* (FBI), 6.4.2004, disponibile al link: *http://www.4law.co.il/L373.pdf*.

HENDERSON J. H., *Public Law Enforcement, Private Security and Citizen Crime Prevention: Competition or Cooperation*, in *Police J.*, 60/1987, p. 48.

ILARDA G., MARULLO G., *Cybercrime: conferenza internazionale*, Giuffrè, 2004.

JAHANKHANI H., JAMAL A., LAWSON S., *Cybersecurity, Privacy and Freedom Protection in the Connected World*, Springer International Publishing, 2021.

JASPER S., *Russian Cyber Operations: Coding the Boundaries of Conflict*, Georgetown University Press, 2020.

JENSEN E., TALBOT E., *Cyber Sovereignty: The Way Ahead*, in *Texas International Law Journal*, 50/2015, p. 275.

JENSEN E., TALBOT E., *The Tallinn Manual 2.0: Highlights and Insights*, in *Georgetown Journal of International Law*, Vol. 48, 2017, p. 735.

JOUGLEUX P., MARKOU C., PRASTITOU T., SYNODINOU T. E., *EU Internet Law in the Digital Era*, Springer International Publishing, 2019.

KENNEY M., *Cyber-Terrorism in a Post-Stuxnet World*, Orbis, 2015.

KLIMBURG A., MIRTL P., *Cyberspace and Governance - A Primer*, in *Austrian Institute for International Affairs* (Oiip), 9/2012, disponibile al link: *http : / / www . oiip . ac . at / publikationen / arbeitspapiere / publikationen – detail / article / 9 2 / cyberspace – and – governance – a – primer . html*.

KONRADOVA N., *The rise of RuNet and the main stages of its History*, in AA.VV., S. DAVYDOV (a cura di), *Internet in Russia A Study of the Runet and Its Impact on Social Life,* Springer, 2020, p. 39.

KOTT A., LINKOV I., *Cyber Resilience of Systems and Networks*, Springer International Publishing, 2019.

LAB S. P., *Crime Prevention. Approaches, Practices, and Evaluations*, Taylor & Francis, 2013.

LAMBERTI C., *Gli strumenti di contrasto al terrorismo ed al cyber-terrorismo nel contesto europeo*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. VIII, n. 2, 5-8/2014, p. 142.

LAMÉRIS F., *Crime Control: A Proposal for The Netherlands*, in *Police Stud. Int'l Rev. Police Dev*., 6/1983-1984, p. 13.

LARINNI C., *Garantismo europeista: un ossimoro? a proposito dell'accesso abusivo ad un sistema informatico o telematico (615-ter c.p.)*, in *DisCrimen*, 29.6.2020.

LAY S., PASCARELLA M., *Hacktivismo, cyberterrorismo e misure di contrasto*, The Alpha Institute of Geopolitics and Intelligence, 2016.

LAVORGNA A., *Cybercrimes*, RED GLOBE Press, 2020.

LEUKFELDT E. R., THOMAS J. H., *The Human Factor of Cybercrime*, Routledge, 2020.

LEVI P., *Se non ora, quando?*, Einaudi, 1982.

LEVITA L., *Reati informatici. Disciplina sostanziale e questioni processuali*, Giuffrè, 2012.

LEVY S., *Hackers: Heroes of the Computer Revolution*, O REILLY, 1984.

LEVY P., *Il virtuale*, Raffaello Cortina, 1997.

LINKOV I., PALMA-OLIVEIRA J. M., *Resilience and Risk. Methods and Application in Environment, Cyber and Social Domains*, Springer Netherlands, 2017.

LUCINI B., *Cyber Resilience e Sicurezza (nazionale): aspetti e considerazioni*, in *ITSTIME*, 2.6.2020, disponibile al link: *https://www.itstime.it/w/cyber-resilience-e-sicurezza-nazionale-aspetti-e-considerazioni-by-barbara-lucini/*.

LUIIJF E., *Definitions of Cyber Terrorism*, in AKHAGAR B., BOSCO F., STANIFORTH A., *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Elviser Science, 2014, p. 11.

LUPARIA L., *Sistema penale e criminalità Informatica*, Giuffrè, 2009.

LUPERTO M., *Gli obblighi dei fornitori di servizi di comunicazione elettronica in caso di violazione dei dati personali (data breach) ed il delitto dell'art. 168, D.lgs. n. 196/2003*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *Cybercrime. Diritto e procedura penale dell'informatica*, UTET, 2019, p. 944.

LYTOARD J. F., *La condizione postmoderna. Rapporto sul sapere*, Feltrinelli, 1985.

MAGGIONI M., MAGRI P. (a cura di), *Twitter e jihad. La comunicazione dell'Isis*, Epoké, 2015.

MAIELLO V., *Le misure di prevenzione dopo il c.d. Codice antimafia. Aspetti sostanziali e aspetti procedurali - profili sostanziali: le misure di prevenzione personali*, in *Giur. It.*, 6/2015, p. 1523.

MANGIARACINA A., *Il "congelamento dei beni" e la confisca come misure di contrasto alla criminalità organizzata transnazionale e al terrorismo*, in AA.VV., *La Giustizia patrimoniale penale*, UTET, 2011.

MANNA A., *Società dell'informazione e diritto penale: problemi e prospettive*, in *Arch. Pen.*, 1/2014, p. 340.

MANNA A., *Misure di prevenzione e diritto penale: una relazione difficile*, IUS PISA, 2019.

MANTOVANI M., *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Crit. del dir.*, 4/1994, p. 18.

MANTOVANI F., *Diritto penale. Parte speciale*, CEDAM, 2019.

MARINI L., *L'evoluzione della disciplina internazionale in materia di terrorismo: qualche spunto recente fra Onu ed Europa*, in *QuestioneGiustizia*, 2/2017, disponibile al link: *https://www.questionegiustizia.it/rivista/articolo/l–evoluzione-della-disciplina-internazionale–in–materia–di-terrorismo_qualche–spunto–recente-fra–onu–ed–europa_452.php*

MARINI L., *Foreign terrorist fighters: verso la revisione della risoluzione 2178 (2014)*, in *Dir. Pen. Comp*., 20.12.2017, p. 4.

MARTINO L., *La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica*, CSSII UNFI, 2012.

MARTINI A., *Essere pericolosi. Giudizi soggettivi e misure personali*, Giappichelli, 2017.

MARTORANA M., *Terrorismo sul web e contenuti online: il nuovo regolamento UE*, in *Altalex*, 25.5.2021, disponibile al link: *https : / / www . altalex . com / documents / news / 2021 / 05 / 25 / terrorismo - web - contenuti - online - nuovo - regolamento – europeo*.

MASARONE V., *Politica criminale e diritto penale nel contrasto al terrorismo internazionale*, Ed. Scientifiche Italiane, 2013.

MASARONE V., *Il "diritto penale europeo" al vaglio dell'offensività: fondamento ed esiti*, in *Arch. Pen.*, 1/2019, p. 18.

MAZZA F., *Una nuova forma di criminalità economica: la pirateria informatica. Orientamenti dell'Unione Europea e strategie di contrasto, in Spunti critici in tema di nuove forme di criminalità*, in AA.VV., *Spunti critici in tema di nuove forme di criminalità*, 2007, p. 40.

MAZZACUVA F., *Le persone pericolose e le classi pericolose*, in S. FURFARO (a cura di), *Misure di prevenzione*, UTET, 2013, p. 110.

MCBEATH G. B., WEBB S. A., *Imagining cities*, Routledge, 2018.

MCQUADE S. C., *Encyclopedia of Cybercrimes*, Greenwood Press, 2009.

MENDITTO F., *Le misure di prevenzione personali e patrimoniali*, Giuffrè, 2019.

MENDITTO F., *Presente e futuro delle misure di prevenzione (personali e patrimoniali): da misure di polizia a prevenzione della criminalità da profitto*, in *Dir. Pen. Cont*., 23.5.2016, p. 23.

MENDITTO F., *La sentenza de Tommaso c. Italia: verso la piena modernizzazione e la compatibilità convenzionale del sistema della* prevenzione, in *Dir. Pen. Cont.*, 4/2017, p. 13.

MERUSI F., *Profili amministrativi delle misure di prevenzione*, in *Centro nazionale di prevenzione e difesa sociale*, *Le misure di prevenzione*, Atti del Convegno «Enrico De Nicola» (Alghero, 26-28 arile 1974), Giuffrè, 1975.

MIDORO V., *Quale alfabetizzazione per la società della conoscenza?*, in *Italian Journal of Educational Technology*, 1.1.2007, disponibile al link: *https : / / www . provinz . bz . it / bildungsprache / sprachen / downloads / Quale _ alfabetizzazione _ per _ la _ soc . _ della _ conoscenza . pdf*,.

MITTAL S., TOLK A., *Complexity Challenges in Cyber Physical Systems. Using Modeling and Simulation (M&S) to Support Intelligence, Adaptation and Autonomy*, Wiley, 2019.

MOORE R., *Cybercrime: investigative high-technology computer crime*, LexisNexis Publication, 2005.

MORELLI F. B., *La giurisprudenza costituzionale italiana tra diritto alla riservatezza e potere di controllo sulle informazioni personali*, in NEGRI D. (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Aracne, 2007, p. 41.

MORO P. (a cura di), *Etica, informatica, diritto*, Franco Angeli, 2008.

MORO P. (a cura di), *Il diritto come processo. Princìpi, regole e brocardi per la formazione critica del giurista*, Franco Angeli, 2014.

MUELLER M., *Sovereignty and Cyberspace: Institutions and Internet governance*, 5th Annual Vincent and Elinor Ostrom Memorial Lecture, University of Indiana, 3.10.2018, p. 3, disponibile al *link*: *https : / / dlc . dlib . indiana . edu / dlc / bitstream / handle / 10535 / 10410 / 5th – Ostrom - lecture DLC . pdf ? sequence = 1&isAllowed = y*.

NARDI V., *La punibilità dell'istigazione nel contrasto al terrorismo internazionale*, in *Dir. Pen. Comp*., 1/2017, p. 120.

NOCETI A., PIERSIMONI M., *Confisca e altre misure ablatorie patrimoniali*, Giappichelli, 2011.

NUVOLONE P., *Relazione introduttiva, in Centro nazionale di prevenzione e difesa sociale*, *Le misure di prevenzione*, Atti del Convegno «Enrico De Nicola» (Alghero, 26-28 aprile 1974), Giuffrè, 1975.

ORLANDI R., *Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici*, in *Arch. Pen.*, 25.7.2016, p. 10.

PADOVANI T., *Stato (reati contro la personalità dello)*, in *Enc. dir.*, Vol. XLIII, 1990.

PADOVANI T., *La pericolosità sociale sotto il profilo giuridico*, in FERRACUTI F. (a cura di), *Trattato di criminologia, medicina criminologica e psichiatria forense*, vol. XIII, Giuffrè, 1990, p. 313.

PADOVANI T., *Diritto penale*, Giuffrè, 2019.

PALAZZO F., *Per un ripensamento radicale del sistema di prevenzione ante delictum*, in *Discrimen*, 12.9.2018, p. 12.

PANAGIA S., *Il delitto politico nel sistema penale italiano*, CEDAM, 1980.

PANNAIN R., *Personalità internazionale dello Stato (delitti contro la)*, in *Noviss. Dig. It.*, vol. XII, 1965, p. 1110.

PARACAMPO M. T. (a cura di), *FinTech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli, 2017.

PARENTE F., *Sistemi cibernetici, autoapprendimento integrale e intelligenza connettiva*, in *Annali del Dipartimento Jonico dell'Università degli Studi di Bari*, EDJzioniSGE, 2018.

PARODI C., SELLAROLI V. (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Giuffrè, 2020.

PASCULLI L., *Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali*, Padova University Press, 2012.

PASCULLI L., *The Global Causes of Cybercrime and State Responsibilities. Towards an Integrated Interdisciplinary Theory*, in *Journal of Ethics and Legal Technologies*, Vol. 2, 4/2020, p. 5.

PASTORELLO M., *How cyberspace is used by terrorist organization: possible threats to critical infrastructures? The most recent activities of cyber counterterrorism*, in *Sicurezza, terrorismo e società*, 2/2015, p. 117.

PAVARINI M., *La pena «utile», la sua crisi e il disincanto: verso una pena senza scopo*, in *Rassegna Penitenziaria e criminologica*, 1/1983, p. 16

PAVARINI M., la voce *Pena*, in *Enciclopedia delle scienze sociali*, Treccani, 1996, al link *https://www.treccani.it/enciclopedia/pena_%28Enciclopedia-delle-scienze-sociali%29/*.

PECORELLA C., *Diritto penale dell'informatica*, CEDAM, 2006.

PECORELLA C., *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo a un sistema informatico o telematico e commento* – nota a Cass. pen., I sez., sent. 27 maggio 2013 (dep. 27 settembre 2013), Pres. Chieffi, Est. La Posta, confl. comp. tra GIP Roma e Trib. Firenze, in *Dir. Pen. Comp.*, 11.10.2013.

PELISSERO M., *Reati contro la personalità dello Stato e contro l'ordine pubblico*, Giappichelli, 2010.

PELISSERO M., *Il vagabondo oltre confine. Lo statuto penale dell'immigrato nello Stato di prevenzione*, in *Politica del diritto*, Vol. II, 2011, p. 239.

PELISSERO M., *Contrasto al terrorismo internazionale e diritto penale al limite*, in *Terr. e dir. pen*., 8/2016, p. 99.

PELISSERO M., *Le "fattispecie di pericolosità": i presupposti di applicazione delle misure e le tipologie soggettive i destinatari della prevenzione praeter delictum: la pericolosità da prevenire e la pericolosità da punire*, in *Riv. It. Dir. Proc*., 2017, p. 439 e ss.

M. PELISSERO, *Diritto penale - Appunti di parte generale*, Giappichelli, 2021.

PERRY K., *Measuring the Effect of Neighbourhood Crime Watch in Lakewood, Colorado*, in *Police J.*, 57/1984, p. 221.

PERSIANI D., *Introduzione alla cibernetica*, Bollati e Beringhieri, 1997.

PEZZUTO R., *Contenuti terroristici on line: l'unione europea lavora a nuove norme per prevenirne la diffusione*, in *Dir. Pen. Comp.*, 4/2019, p. 38.

PIATTOLI B., *Principio di proporzionalità UE e trattamento dei dati personali nella lotta al terrorismo*, in *Dir. Pen. e Proc.*, 7/2015, p. 885.

PICA G., *Diritto penale delle tecnologie informatiche*, UTET, 1999.

PICA G., *Reati informatici e telematici*, UTET, 2000.

PICOTTI L., *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*, CEDAM, 2004, p. 21.

PICOTTI L., *Reati informatici, riservatezza, identità digitale*, *AIDP*, 2004.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, in *Dir. Pen. e Proc.*, 6/2008, p. 696.

PICOTTI L., ZANUSO F. (a cura di), *L'antropologia criminale di Cesare Lombroso dall'Ottocento al dibattito filosofico-penale contemporaneo*, Edizioni Scientifiche Italiane, 2011.

PICOTTI L., *Tutela penale della persona e nuove tecnologie*, CEDAM, 2013.

PICOTTI L., *Quale diritto penale nella dimensione globale del cyberspace*?, in AA.VV., R. WENIN, G. FORNASARI (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali,* ed. Università degli Studi di Trento, 2017, p. 310.

PINO R., *Il "cyberterrorismo": un'introduzione,* in *Ciberspazio e diritto: rivista di informatica giuridica*, 3/2013, p. 430.

PITTARO P., *La natura giuridica delle misure di prevenzione*, in AA.VV., F. FIORENTIN (a cura di), *Misure di prevenzione personali e patrimoniali*, Giappichelli, 2018, p. 143.

PIVA D., *La responsabilità degli enti ex d.lgs. 231/2001 tra diritto e processo*, Giappichelli, 2021.

PIZZETTI F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018.

PLATONE (trad. a cura di M. MIGLIORI), *Politico*, Bompiani, 2001.

POKALOVA E., *Returning Islamist Foreign Fighters. Threats and Challenges to the West*, Springer, 2019.

POLLIT M., *Cyberterrorism- Fact or Fancy?*, in *Computer Fraud & Security*, 8/1997, p. 8.

PULITANÒ D., *Relazione di sintesi. Misure di prevenzione e problema della prevenzione,* in *Riv. it. dir. proc. pen*., 2/2017, p. 635.

PURDY E. R., *Cyberterrorism,* Salem Press Encyclopedia, 2019.

RECCHIONE S., *La pericolosità sociale esiste ed è concreta: la giurisprudenza di merito resiste alla crisi di legalità generata dalla sentenza "De Tommaso v. Italia" (e confermata dalle sezioni unite "Paternò")*, commento a Trib. Roma, sez. specializzata misure di prevenzione, decr. 3 aprile 2017, n. 30 (con memoria depositata dalla Procura della Repubblica di Tivoli) e a Trib. Palermo, Sez. I – misure di prevenzione, decr. 1 giugno 2017, n. 62, in *Dir. Pen. Cont*., 10/2017, p. 133.

RECCIA E., *L'aggravante ex art. 7 d.l. n. 152 del 13 maggio 1991: una sintesi di "inafferrabilità del penalmente rilevante"*, in *Dir. Pen. Cont*., 2/2015, p. 252.

RESTA F., *Virtualità del crimine. Dai reati informatici ai cybercrimes*, in *L'informatica del diritto*, in *Giur. Merit.*, 11/2006, p. 102.

RESTIVO C., *Contributo ad una teoria dell'abuso del* diritto, Giuffrè, 2007.

RIONDATO S., *Un diritto penale detto "ragionevole". Raccontando Giuseppe Bettiol*, CEDAM, 2006.

RIONDATO S., *Le misure di prevenzione e il degrado delle garanzie delle garanzie annunciato da Giuseppe Bettiol*, in AA.VV. (a cura di S. RIONDATO), *Dallo Stato Costituzionale Democratico di ritto allo Stato di polizia*, Padova University Press, 2012, p. 117.

ROBERTO S., *La protezione delle Infrastrutture Critiche informatizzate*, in *Automazione e Strumentazione*, 8/2003, p. 27.

ROCCATAGLIATA L., *Da Strasburgo: la misura di prevenzione della sorveglianza speciale di pubblica sicurezza viola al Convenzione EDU (Sentenza De Tommaso)*, in *Giur. Pen. web*, 24.2.2017.

ROCCO A., *Politica e diritto nelle vecchie e nuove concezioni dello Stato*, Nuova Antologia, 1937.

RODOTÀ S., *Discorso del Presidente Stefano Rodotà*, nella *Relazione annuale del Garante della Privacy*, 2004.

RODOTÀ S., *Persona, libertà, tecnologia. Note per una discussione*, in *Diritto & Questioni pubbliche*, 5/2005, p. 25.

RONCO M., *Il significato retributivo-rieducativo della pena*, in *Dir. Pen. e Proc*., 2/2005, p. 137.

RONCO M. (a cura di), *Persone e sanzioni. Presupposti soggettivi, previsione, comminazione ed esecuzione delle sanzioni penali*, Zanichelli, 2010.

RONCO M., *Appunti di diritto penale*, Libreria Progetto Padova, 2014.

ROSS J. I., *Cybercrimes*, Chelsea House, 2010.

RUGGE F., *Mind hacking: la guerra informativa nell'era cyber,* in *Notizie di Politeia*, XXXIV, vol. 132, 2018, p. 118.

SABELLA P. M., *Il fenomeno del cybercrime nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali*, in *Informatica e diritto*, Vol. XXVI, 1/2017, p. 139.

SALUZZO S., SPAGNOLO A., *La responsabilità degli Stati e delle organizzazioni internazionali nuove fattispecie, problemi di attribuzione e di accertamento*, Ledizioni, 2018.

SALVADORI I., *Hacking, cracking e nuove forme di attacco ai sistemi di informazione. Profili di diritto penale e prospettive de iure condendo*, in *Ciber. Dir.*, 9/2008, p. 344.

SALVADORI I., *L'accesso abusivo ad un sistema informatico o telematico, una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in PICOTTI L. (a cura di), *Tutela penale delle persone e nuove*, CEDAM, 2013, p. 125.

SALVADORI I., *Il diritto penale dei software a duplice uso,* in AA.VV., R. WENIN, G. FORNASARI (a cura di)*, Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali, ed. Università degli Studi di Trento, 2017*, p. 361.

SANFILIPPO G., *Diritto penale – Parte generale*, Key, 2022.

SANTINI S., *L'Europa compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, in *Dir. Pen. Comp*., 7-8/2017, p. 14.

SARZANA DI S. IPPOLITO C., *L'accesso illecito alle banche dati ed ai sistemi informatici pubblici*, in *Dir. Inf*., 2007, p. 277.

SARZANA DI S. IPPOLITO C., *Informatica, internet e diritto penale*, Giuffrè, 2010, p. 773.

SCHNEIDER S., *Crime Prevention. Theory and Practice*, Taylor & Francis, 2014.

SELLAROLI V., *Il nuovo reato di cyberbullismo (l. 29 maggio 2017, n. 71)*, Giuffrè, 2017.

SEREDYŃSKA I., *Insider Dealing and Criminal Law. Dangerous Liaisons,* Springer Berlin Heidelberg, 2011.

SERENI A., *Delitti contro la personalità dello Stato*, in FIORELLA A. (a cura di), *Questioni fondamentali della parte speciale del diritto penale*, Giappichelli, 2019, p. 543.

SHANY Y., *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, in *The American Journal of International Law*, vol. 112, 4/2018, p. 583.

SIEBER U., *International cooperation against terrorist use of the Internet*, in *Eres*, 3/2006, p. 395.

SILVESTRI G., *L'individuazione dei diritti della persona*, in *Dir. Pen. Cont*., 29.10.2018, p. 8.

SIRACUSANO F., *La tassativizzazione delle fattispecie di pericolosità per la sicurezza pubblica tra paradigmi convenzionali e garanzie costituzionali*, in *Arch. Pen*., 1/2022, p. 10.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA (SISR), *Relazione annuale 2021*, p. 20, 84, disponibile al link: *https://www.sicurezzanazionale.gov.it/sisr.nsf/wpcontent/uploads/2022/02/RELAZIONE-ANNUALE-2021.pdf*.

SODDU M., *Terrorismo, pericolosità sociale e recidiva*, Pacini Giuridica, 2016.

SPOENLE J., *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Discussion paper*, Council of Europe, Strasbourg, 2010.

STASIO D., *La lotta multilivello al terrorismo internazionale*, Giuffrè, p. 242.

STEA G., *La responsabilità penale dell'internet provider*, nota a Cass. Pen., Sez. V, 1 marzo 2016 (ud. 13 luglio 2015), n. 8328, in *Giur. Pen*., 11/2016, p. 4.

SUN T. (trad. it. a cura di CONTI M.), *L'arte della guerra*, Feltrinelli, 2013, Cap. III, vers. 18.

TADDEO M., *Is Cybersecurity a Public Good?*, in *Minds & Machines*, 29/2019, p. 354.

TAKALA H., *Nordic Cooperation in Criminal Policy and Crime Prevention*, in *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 5/2004, p. 131.

TALIHÄRM A. M., *Cyberterrorism: in theory or in practice?*, in *Defence Against Terrorism Review*, 2/2010, p. 63.

TILLEY N., *Handbook of Crime Prevention and Security Safety*, Willan Publishing, 2005.

TORRE M., *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali,* in *Dir. Pen. e Proc.,* 9/2015, p. 1163.

TRAPANI M., *Guerra e diritto penale. Sull'adeguatezza degli strumenti penalistici nei confronti del c.d. terrorismo islamico*, in AA.VV., *Politica criminale e cultura giuspenalistica*. *Scritti in onore di Sergio Moccia*, Jovene, 2017, p. 253.

UDA R. T., *Cybercrime, Cyberterrorism, and Cyberwarfare*, Xilibris, 2009.

URICCHIO G., *Guerra Russia-Ucraina, l'intervento di Anonymous e la cybersecurity*, in *Altalex*, 1.3.2022, disponibile al *link*: *https://www.altalex.com/ documents/news/2022/03/01/guerra–russia–ucraina–intervento–di– anonymous– e–la–cybersecurity*.

VALENTINI V., *Diritto penale intertemporale: logiche continentali ed ermeneutica europea*, Giuffrè, 2012.

VALITUTTI D., *I delitti contro la personalità dello Stato tra delitto politico e diritto penale del nemico: una ricostruzione critica*, Il Mulino, 2015.

VALSECCHI A., *Brevi osservazioni di diritto penale sostanziale*, in *Dir. Pen. Proc.*, 10/2005, p. 1226.

VALSECCHI A., *Addestramento ad attività con finalità di terrorismo anche internazionale" (art. 270 quinquies c.p.): la prima pronuncia della cassazione,* nota a Cass. pen., Sez. VI, sent. 20.7.2011 (dep. 25.7.2011), n. 29670 - Pres. e Rel. De Roberto, in *Dir. Pen. Cont*., 20.12.2011.

VALSECCHI A., *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 Trib. Firenze (GIP), ord. 9.1.2013, (Pezzuti), in *Dir. Pen. Cont*., 21.2.2013, p. 3.

VALSECCHI A., *Attacco «no T.a.v.» e attentato per finalità terroristiche: la Cassazione fissa le coordinate fondamentali per l'interprete*, in *Quest. giust*., 3/2014, p. 229.

VENEZIANI P., *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in *Ind. Pen*., 1/2000, p. 139.

VERONESI P., *Per un'interpretazione costituzionale del concetto di "domicilio"*, in *Ann. Univ. Ferrara*, XVII, 2003, p. 125.

VIGANÒ F., *Terrorismo, guerra e diritto penale*, in *Riv. It. dir. proc. pen*., 4/2006, p. 694.

VIGANÒ F., *La nozione di terrorismo ai sensi del diritto penale*, in SALERNO F. (a cura di), *Sanzioni individuali del Consiglio di Sicurezza e garanzie processuali fondamentali*, CEDAM, 2010.

VIGNERI A. F., *Cyberterrorismo: realtà o finzione? Profili problematici di definizione e contrasto*, in *Opinio Juris*, 3.9.2018, p. 8.

VIGNERI A. F., *Brevi considerazioni sulla natura e sulle caratteristiche dello spazio cibernetico*, in *SalvisJuribus*, 10.10.2019 disponibile al link: *http : / / www . salvisjuribus . it / brevi – considerazioni – sulla – natura – e –sulle – caratteristiche – dello – spazio – cibernetico /.*

VON HEINEGG W. H., *Chapter 1: The Tallinn Manual and International Cyber Security Law*, in *Yearbook of International Humanitarian Law*, vol. 15, 2012.

WEBB M. (foreword by DOCTOROW C.), *Coding democracy. How Hackers are distrupting power, surveillance and authoritarianism*, The MIT Press, 2020.

WELSH B. C., ZANE S. N., ZIMMERMAN G. M., *Examining the Historical Developments and Contemporary Relevance of the Longitudinal–Experimental Design of the Cambridge-Somerville Youth Study: Utility for Research on Intergenerational Transmission of Offending*, Springer International Publishing, 2016.

WIENER N., *Cybernetics, or control and communication in the animal and the machine,* The MIT Press*,* 1948.

WIENER N., *The human use of human beings*, Houghton Mifflin, 1953.

ZACCHIA A., *Osservazioni a Cass. Pen., Sez. VI, n. 28009, 15 maggio 2014*, in *Cass. pen*., 3/2015, p. 1115.

ZEMBA V., *Defining, measuring, and enhancing resilience for small groups*, in *Safety Science*, 12/2019, p. 603.

ZIRULIA S., *Apologia dell'IS via internet e arresti domiciliari. Prime prove di tenuta del sistema penale rispetto alla nuova minaccia terroristica* (nota a Cass., pen., Sez. I, sent. 6.10.2015, n. 47489), in *Dir. Pen. Comp*., 14.12.2015.

ZOLLI A., *Resilienza*, Rizzoli, 2017.