UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Privato e Critica del Diritto

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea Magistrale in

Giurisprudenza

Anno Accademico 2022/2023

L'associazione per delinquere operante online: profili criminologici e penali

Relatore: Chiar.ma Prof. Debora Provolo

Studente: Eugenia Maria Andolina

Matricola: 1119217

A nonno Franco,

nonna Fanina,

nonna Pinuccia,

e a nonno Giovanni,

che sorrideranno e canteranno dall'alto

vedendomi.finalmente con la corona in testa..

.

INDICE

Capitolo I- L'Associazione per delinquere. I profili di maggior criticità nella frattispecie.

Capitolo II - Il fenomeno del Cybercrime.

Capitolo III - L'associazione a delinquere online

Capitolo I: L'associazione per delinquere. I profili di maggior criticità nella fattispecie.

1. L'interesse tutelato: la difficile individuazione del concetto di ordine pubblico

Risulta esser indubbio che il bene giuridico tutelato dall'art.416 c.p. è l'ordine pubblico. Tuttavia, prima di procedere nell'analisi di diversi elementi della fattispecie, è necessario soffermarsi brevemente sulla sua definizione in relazione alla fattispecie criminosa in esame.

Innanzitutto, è necessario precisare che non si farà riferimento in questa sede all'accezione di ordine pubblico intesa dal Codice Civile[1], né a quella, impiegata nel diritto pubblico, di ordine pubblico di polizia[2].

Piuttosto, nell'ambito di questa trattazione, bisognerà delineare l'ordine pubblico in relazione alla società democratica, descrivendolo come una <<situazione di pacifica convivenza senza la quale qualunque società si disgrega>>[3].

Facendo un breve inquadramento storico, il legislatore del 1930 ha introdotto l'art. 416 c.p. in sostituzione dell'art 248 del Codice Zanardelli (rimuovendo, in particolare, il riferimento alle specifiche ipotesi di delitti-scopo in grado di sovvertire l'ordine politico e sociale), sia perché non si poteva ignorare l'aperta emersione dei nuovi fenomeni di organizzazione criminale di carattere mafioso, ma anche perché presente l'esigenza nel regime fascista di reprimere quelle forme di associazionismo in grado di minacciare la stabilità del regime politico in questione.[4]

---

[1] Corso, *Ordine pubblico(dir. pubbl.)*, in *Enciclopedia del Diritto,* Vol. XXX, Giuffrè,1980, pag.1058, identifica che quest'accezione di ordine pubblico consiste in << *un limite di efficacia agli atti giuridici di uno Stato estero* [legge, sentenza, atto amministrativo, n. d. a.] *o alle manifestazioni di autonomia negoziale dei privati*>>,

[2] Corso,*op. cit.*, pag. 1079, la delinea come: <<*l'interesse che autorizza interventi dell'autorità di pubblica sicurezza*>>.

[3] *Ivi*, pag.1083.

[4] Dolcini, *Appunti su Criminalità organizzata e reati associativi*, in *Arch. Pen.,* 1982, pag. 263, dove identifica che si << sottovalutava il rischio, per il nuovo regime autoritario, del riemergere di associazioni politiche tendenti al ristabilimento della democrazia, e la conseguente esigenza di tutelare il regime attraverso un adeguato sistema di incriminazioni>>..Per maggiori approfondimenti sul quadro storico, cfr.: Aleo, *Sistema Penale e criminalità organizzata. Le figure delittuose associative*, 1999, Giuffrè,pag. 54 e ss. .

Ciò permette infatti di delineare come il legislatore di quel tempo già si trovasse a fronteggiare la criminalità organizzata, comportando la necessaria formulazione di diverse fattispecie penali (art.416 c.p. compreso, oggetto della nostra trattazione) in contrasto a quel fenomeno tutt'ora presente in diverse sfaccettature ed in costante evoluzione e che va a ledere, appunto, l'ordine pubblico.

Il punto che bisogna affrontare sin dall'inizio, però, è notare come non vi sia nella Costituzione una nozione chiara e definita del concetto di ordine pubblico: perciò, nonostante la breve definizione data precedentemente, è necessario soffermarsi meglio sul significato da dare al concetto dell'ordine pubblico come bene giuridico tutelato dall'articolo 416 c.p.

La nozione di ordine pubblico è una questione complessa e da non sottovalutare: complessa, perché è un concetto facile da capire ma difficile da definire specificamente a livello normativo, da non sottovalutare perché dal diverso significato dato al concetto di ordine pubblico dipende la qualificazione della fattispecie di associazione per delinquere come reato di danno o come reato di pericolo.

Non a caso l'ordine pubblico è stato definito come <<un prisma dalle molteplici sfaccettature>>[5], dove ciascun aspetto ha una propria importanza:

- da un lato, l'ordine pubblico corrisponde ad uno stato psicologico individuale, corrispondente alla sicurezza dello svolgersi della vita sociale in maniera ordinata ed onesta,
- dall'altro lato, l'ordine pubblico ha una sua dimensione tangibile e concreta: può assumere il significato di pacifica e sicura convivenza collettiva, ma anche sfociare nel corretto ed imparziale funzionamento dei meccanismi amministrativi ed istituzionali, ovvero al corretto funzionamento delle attività finanziarie ed economiche.

Considerata la natura della associazione a delinquere, che – proprio per il fatto che nasca, si sviluppa e si inserisca nella società civile- essa è in grado di turbare non solo la tranquillità individuale e collettiva, ma anche arrivare a minacciare lo stesso Stato; si deve necessariamente conseguire che una mera connotazione <<psicologica>> dell'ordine

[5] Antonini, *Le Associazioni per delinquere nella Legge Penale Italiana*, in *Giust. Pen*., 1985, p.315.

pubblico risulti essere del tutto parziale ed incompleta[6], perché tale da disperdere ulteriormente <<il fluttuante spessore oggettivo>>[7] del concetto stesso di ordine pubblico.

Da queste premesse, si può desumere quindi l'emersione di tre aspetti fondamentali e coesistenti nella nozione dell'ordine pubblico: da un lato, una dimensione sovraindividuale dell'ordine pubblico, dall'altro lato una dimensione emotiva e di una dimensione empirica, tutti e tre impossibili da ignorare. Nell'esplorare la tematica in questione, è quindi necessario tener contemporaneamente in considerazione tutte queste tre diverse dimensioni.

Nella dottrina sul tema[8], si trovano individuate due principali accezioni del concetto di ordine pubblico,il c.d. ordine pubblico <<ideale>> e l'ordine pubblico <<materiale>>. Vi è un'ulteriore e particolare nozione di ordine pubblico, definita da Iacoviello come la c.d**.** <<concezione ordinamentale >>[9] di ordine pubblico.

Bisognerà affrontare queste tre diverse posizioni nel dettaglio.

1. Trattando l'ordine pubblico come <<ideale>>, per esso s'intende l'insieme dei principi e i valori fondamentali dell'ordinamento necessari per la sua esistenza ed il suo perdurare (in sostanza, si tratterebbe quindi dell'ordine legale costituito) [10] . Se si seguisse quest'accezione di ordine pubblico, sarebbe necessaria una concreta situazione di pericolo per la collettività. [11]

   Tra i vari autori e le pronunce a sostegno della posizione[12], si cita brevemente la posizione di Dolcini, il quale, rispetto a questo concetto di ordine pubblico <<ideale>> rileva la sua <<idoneità classificatoria>>[13], in quanto in grado di nobilitare tutto l'insieme delle norme

---

[6] Nello stesso senso:, Iacoviello,*Ordine Pubblico e Associazione per Delinquere*, in *Giust. Pen.,* 1990, II, pag. 52. *Contra*: Manzini, *Trattato di Diritto penale italiano*, (agg. a cura di)Nuvolone, Pisapia, UTET, 1983, pag 158.

[7]Antonini, *op. cit.,*p.315.

[8]Per una panoramica generale sulle diverse posizioni dottrinali v. Borsari e Provolo, *Associazione per delinquere*, in Fornasari et al., *Reati Contro l'ordine pubblico*, Giappichelli, 2017, pagg.31-32.

[9]Iacoviello, *op .cit.,* pag.43.

[10] Borsari e Provolo, *op. cit*., pag.31.

[11] Corte Cost. n.65/1970; in *Giur. Cos*t, 1970, pag. 955; Corte Cost. n. 199/1972, in *Giur. Cost*., 1972, pag. 2218.

[12]A sostegno della nozione di ordine pubblico <<ideale>>, oltre a quelli che verranno menzionati,si cita : Fiore, voce *Ordine Pubblico (pen.),* in *Enciclopedia del Diritto*, Volume XXX, ,Giuffrè, 1980, pagg. 8-9. Per la giurisprudenza: Corte Cost., n.19/1962, in *Giur. Cost*, pag. 189.

[13]Dolcini ,*op. cit.* pag. 279.

giuridiche sottostanti l'ordinamento come un interesse giuridico da proteggere contro la criminalità organizzata[14].

La nozione in esame ha suscitato tuttavia critiche da parte della dottrina,prendendo come riferimento la posizione di Insolera.

Egli denota una serie di problematiche nell'accogliere questa configurazione dell'ordine pubblico come <<ideale>>.*In primis*, egli fa una critica di carattere tecnico, sottolineando l'eccessiva fluidità del termine: il concetto non è capace di distinguersi rispetto alle tematiche di tutela, riducendosi ad esser solo una <<fotografia di un assetto normativo già dato>>[15].

Ma non è la sola contestazione che muove a questa concezione: lui esclude pure un ulteriore significato del concetto di ordine pubblico ideale, il c.d. <<ordine pubblico normativo>>,[16] ossia l'insieme dei principi non codificati e non giuridici (ad esempio etici, politici, economici) che si devono seguire per assicurare il mantenimento dell'ordine costituzionale. Prendendo come riferimento la posizione di Lavagna[17], egli fa notare che, qualora venisse accolta questa accezione di ordine pubblico, si creerebbero delle difficoltà nello stesso esercizio di potere dell'autorità pubblica, la quale potrebbe esercitare dei poteri legati ad una visione ideologica, ma allo stesso tempo con discrezionalità: cosa non solo impensabile, se si pensa alla stessa natura del bene pubblico; ma pure configurante un profilo di abuso di potere pubblico[18].

In conclusione, Insolera afferma che l'ordine pubblico non può esser considerato come un valore della Costituzione o bene suscettibile di tutela penale senza esser collegato alle esigenze <<di pubblica incolumità, sicurezza, salute e tranquillità>>[19] dell'ordinamento.

In linea a quest'ultimo pensiero è anche Iacoviello, secondo il quale qualsiasi bene giuridico da tutelare mediante la norma penale deve avere le caratteristiche della concretezza e percettibilità: deve esserci l'effettiva conoscibilità e percezione della

[14]*Ibidem,* delinea ciò come una delle argomentazioni a fondamento della sua proposta, indicata nella stessa pag., di eliminare il titolo rivolto ai <<delitti contro l'ordine pubblico>> e alla loro parziale ricollocazione nel titolo rivolto ai <<delitti contro la personalità dello Stato>>.
[15]Insolera, *L'associazione per delinquere*, CEDAM, 1982, p.161. Nello stesso senso: De Vero, *Istigazione, libertà di espressione e tutela dell'ordine pubblico,* in *Arch. Pen.,* 1976, vol. II, pag. 10; Lavagna, *Il concetto di ordine pubblico alla luce delle norme costituzionali,* in *Dem. e Dir.*, 1967, vol. 3-4, p. 366 e ss.
[16]Insolera, *op .cit.,* pag.164.
[17]Lavagna, *op. ci*t., pag.373.
[18]Insolera, *op. cit,* pag. 164. Nello stesso senso: Lavagna, *op. cit.,* pag. 372; Pace, *Il concetto di ordine pubblico nella Costituzione Italiana,* in *Archivio Giuridico "Filippo Serafini"* ,XXIV, 1963, pag. 117.
[19]Insolera, *op. cit,,* pag. 166. Nello stesso senso: Lavagna, *op. ci*t., pag.362.

possibile offendibilità del bene giuridico. In altre parole , il bene giuridico dev'essere ben << radicato nell'esperienza sociale>>[20].

Da questo breve inciso si può individuare, dunque, come *fil rouge* di queste critiche alla nozione di ordine pubblico ideale, l'eccessiva indeterminatezza del bene giuridico oggetto di tutela.[21]

2. La seconda posizione (che risulta esser la posizione maggioritaria della dottrina[22]) è quella della nozione empirico-materiale, che identifica l'ordine pubblico come il <<buon assetto ed il regolare andamento del vivere civile>>[23].

   A sostegno di questa concezione si pone Insolera: riprendendo i pensieri di Pace e Zuccalà nella sua opera, egli definisce l'ordine pubblico come <<lo stato di concreta, tangibile, esteriore, pace, sociale>>[24], nonché << […] sintesi di ciò che serve affinché nei cittadini si instauri un senso collettivo di disciplina, tranquillità, sicurezza>>[25]. Tuttavia, egli chiarisce come per questo concetto di ordine pubblico materiale debbano esser effettuati alcuni accorgimenti:

   a) è necessario che vi sia l'espresso riferimento a fatti precisi e ben circostanziati[26];
   b) L'ordine pubblico deve comunque manifestarsi << nell'astensione dei consociati da fatti penalmente rilevanti>>[27]: citando De Vero, Insolera precisa che solo in questo modo l'incriminazione della condotta da perseguire penalmente risulta saldamente ancorata ad <<[…] una dimensione di "ordine" di carattere sicuramente materiale>>[28].
   c) Infine, si denota come sia possibile una rischiosa evoluzione dell'ordine pubblico materiale, in seguito alle tendenze della politica criminale: da un concetto analizzabile e definibile da un punto di vista tecnico-giuridico,vi è infatti la possibilità che l'ordine

[20]Iacoviello, *op. cit.* , pagg. 45-6. Nello stesso senso: *Relazione ministeriale sul Progetto del codice penale*, in *Lavori preparatori del codice penale e del codice di procedura penale,* parte II, 1929, Ministero della Giustizia e degli affari di culto, pagg. 202-203.
[21]Cfr. : Lavagna, *op. cit*., pagg. 366-367; Antonini, *op. cit*.,pag. 317, Corso, *op. cit.,* pag. 439; Iacoviello (vedi in seguito, pagg.7-8 di questo elaborato).
[22]Tra le varie tesi a sostegno della posizione, si cita:Lavagna, *op. cit*. pag. 366; Pace, *op. cit*., pag. 118; Insolera, *op. cit.,* pag. 168.
[23] Borsari; Provolo, *op. cit*., pag. 32.
[24]Insolera,*op. cit*., pag. 160, fa diretto riferimento a : Pace, *op. cit*., pag.113.
[25] *Ibidem*, richiama in proposito le parole di: Zuccalà, *Personalità dello Stato, ordine pubblico e tutela di libertà di pensiero,* in *Riv. It. Dir. Proc. Pen.* 1966, pag.1171.
[26]Insolera, *op. cit.,* pag. 166. Nello stesso senso: Lavagna, *op. cit.,* pag. 372.
[27]*Ibidem.*
[28]Insolera fa diretto riferimento a : De Vero, *op. cit*., pag. 10. Cfr. anche: Pace, *op. cit.,* pag. 118.

pubblico si trasformi in un <<movimento centrale nell'indirizzo politico e delle scelte istituzionali che vi si collegano>>[29]: questo perché si deve sottolineare la tendenza a rendere l'ordine pubblico, in base ad una scelta di politica criminale, da un oggetto di tutela a scopo dell'intero ordinamento.

Bisogna poi soffermarsi sull'analisi critica che Iacoviello svolge sulla posizione appena illustrata. Seppur egli noti come, tramite questa posizione percepente l'ordine pubblico come <<realtà oggettiva, percepita e vissuta come tale da ogni soggetto sociale>>[30], si riesca a cogliere una duplice dimensione: <<l'aspetto oggettivo>>, dato dall'ordinario svolgersi della vita sociale e <<l'aspetto soggettivo>> (comprensivo sia della componente intellettiva che di quella psicologica)[31], caratterizzato dall'opinione e dal senso di della ritmicità della vita quotidiana , vi sono per lui non pochi elementi che comportano alcune riflessioni critiche.

In primis, per quanto riguarda il dato oggettivo, egli rileva che la definizione è eccessivamente vaga, in quanto il dato stesso non solo non ha uno specifico collocamento nello spazio e nel tempo, ma non viene descritto nemmeno come si manifesta.
Andando nello specifico riguardo le dimensioni spazio-temporali, non si comprende bene se <<il buon assetto>> e <<il regolare andamento del vivere civile>> riguardino la sola comunità del luogo del commesso reato o si estendano all'intera comunità nazionale[32], nonchè se questi termini facciano riferimento al momento del commesso reato, ovvero <<all'intero arco temporale di vigenza della norma>>[33].
Inoltre, parrebbe presente l'utilizzo di un linguaggio avente un tono più persuasivo che descrittivo, in grado di esprimere dei giudizi di valore.

In conclusione, per Iacoviello, <<l'ordinario svolgersi della vita sociale>> non è uno specchio della realtà sociale, ma corrisponde piuttosto all'<<aspettativa diffusa della collettività>>[34]: per lui, è questo l'aspetto che ha una vera e propria dimensione reale.
Di conseguenza, rispetto al concetto de <<il buon assetto o il regolare andamento dell'assetto del vivere civile>> si dovrebbe o individuare uno standard medio che possa esser da strumento di valutazione delle conseguenze causate dal reato commesso alla

[29]Fiore, voce *Ordine Pubblico,* in *Enciclopedia del Diritto*, Volume XXX, Giuffrè,1980, pag.1102.
[30]Iacoviello, *op. cit.,* pag.47.
[31]Pace, *op. cit.,* pag.113.
[32]*Ibidem.*
[33]*Ibidem.*
[34]*Ibidem.*

società, oppure, piuttosto, pensare proprio ad abbandonare l'idea di utilizzare questo concetto, poiché in realtà esso altro non è se non una <<proiezione ideale della coscienza collettiva>>[35].

Per quanto riguarda invece l'aspetto soggettivo, Iacoviello identifica la complessità nel ricondurre ad un livello collettivo l'opinione ed il senso di sicurezza, sentimenti propri del singolo. Infatti, ogni esperienza psicologica, sia individuale che sociale, per essere verificabile deve pur sempre collocarsi in un contesto storico e sociale tangibile .
É quindi evidente per lo studioso come questo concetto dell'ordine pubblico materiale risulti di fatto ancora non esser dotato di dati del tutto chiari, in quanto <<nel suo nucleo logico rimane fascinosamente inesprimibile>>[36].

3. Un'ultima posizione (seppur minoritaria) da tenere in considerazione in riferimento all'ordine pubblico tutelato dall'art.416 c.p., corrisponde alla summenzionata concezione ordinamentale. Secondo Patalano, l'ordine pubblico infatti consisterebbe ne <<l'insieme delle condizioni giuridiche che assicurano la realizzazione della vita associata>>[37].
   Di conseguenza, l'ordine pubblico corrisponderebbe ad una vera e propria istituzione statutale, in quanto l'ordine pubblico non è altro se non <<le condizioni giuridiche di esistenza dell'ordinamento statuale medesimo>>[38], il quale vede negata la sua unicità ed esclusività come ordinamento giuridico dalla stessa esistenza dell'associazione a delinquere semplice.

   A sostegno della posizione risulta esservi Antonini: questo perché secondo lei, grazie a questa nozione, si comprendono le ragioni per cui il concetto di ordine pubblico abbia assunto nel corso degli anni sfumature diverse che, hanno comportato, di conseguenza, l'attribuzione di numerose e differenti definizioni[39].

   Tuttavia, anche per questa concezione di ordine pubblico non sono mancate le critiche.

   La prima, forse di più immediata percezione, è quella sottolineata da Borsari e da Provolo: nella loro trattazione dell'associazione a delinquere, affermano chiaramente come, con

[35]*Ibidem.* Cfr. anche: Grosso, *Le fattispecie associative: Problemi politici e di dommatica criminale*, in *Riv. It. Dir. Proc. Pen.* 1992, vol. I, pagg.416-7.
[36]*Ibidem.,* pag.48..
[37]Patalano, *L'associazione per delinquere*, 1971, Jovene, pag.181.
[38]*Ibidem*, pag.359.
[39]Antonini, *op. cit.,* p.316

questa concezione, si eguaglierebbe il concetto d'ordine pubblico all'intero sistema, esprimendo dunque una nozione di ordine pubblico ideale[40].

La seconda è quella invece sollevata da Iacoviello, che si sofferma di più sulla problematica dell'applicazione di questa concezione alla prassi quotidiana. Egli infatti pone chiaramente all'attenzione che questa nozione non sarebbe adatta per i casi di associazione a delinquere più settoriali. Per fare un esempio concreto, dire che tre o più persone, che si riuniscano e si organizzano per commettere una serie indeterminata di furti oppure per spaccio di eroina, siano << contro le <<strutture essenziali>> dell'ordinamento statale al quale muovono <<guerra>>>>[41], è affermazione <<[…] suggestivamente epica ma difficilmente utilizzabile […] tutti i giorni>>.[42]

Da queste diverse concezioni di ordine pubblico dipende la qualificazione dell'art 416 c.p. come reato di danno o come reato di pericolo.
Anche questa distinzione non è da poco: bisogna ricordare che mentre per il reato di danno è sufficiente l'accertamento della lesione del bene; nel reato di pericolo aumenta lo spazio di discrezionalità del giudice nell'individuazione dell'effettiva presenza del pericolo.
È vero che coloro che nella dottrina accolgono la tesi dell'ordine pubblico in senso materiale tendono a classificare l'art 416 c.p. come una fattispecie di reato di pericolo; mentre chi sostiene l'ordine pubblico inteso come concezione ordinamentale tende a classificarlo come reato di danno[43].

Giusto per citare alcuni esempi:

- Patalano, identifica il bene giuridico dell'art 416 c.p. nell'ordine pubblico inteso come <<ordinamento giuridico penale>>[44]. Nello specifico, la fattispecie dell'associazione a delinquere semplice combatte l'<<istituzione criminale>>[45], elemento non solo integrante l'evento del reato in questione, ma anche capace di dar vita ad un ordinamento giuridico

[40]Borsari;Provolo,*op. cit*., pag. 32
[41]Iacoviello, *op. cit.* pag. 48.
[42]*Ibidem.*
[43]Borsari, Provolo, *op. cit*.,pag. 32.
[44]Patalano, *op. cit.,* pag. 116.
[45]*Ibidem*.

antietico e contrastante all'ordinamento giuridico statale.[46] . Di conseguenza, per Patalano l'art.416 c.p. è necessariamente un reato di danno.

- Insolera, che invece accoglie la nozione di ordine pubblico materiale, critica ampiamente la tesi di Patalano, in due punti in particolare.
  In primo luogo, egli individua che la tipologia di pericolo dato dall'esistenza dell' associazione possa configurare una tipologia di pericolo differente rispetto a quello relativo alle singole fattispecie di pericolo[47].
  Insolera si sofferma poi anche sul fatto che nel caso dell'associazione a delinquere la lesione del bene protetto può esser di maggiore entità, anche se in via potenziale: se la fattispecie facente parte del programma del sodalizio esprime una maggiore pericolosità <<in direzione "verticale">>[48](nel senso della probabilità che dalla sua realizzazione possa conseguire un danno per il bene tutelato); nel caso dell'ipotesi associativa il danno ha invece <<una dimensione orizzontale particolarmente grave >>[49].
  Perciò, visto che l'ordine pubblico materiale per Insolera è una <<concreta, tangibile pace sociale>>[50], essa viene vista da quest'ultimo come un bene giuridico che, a livello costituzionale, si trova in una posizione più elevata rispetto ai beni giuridici che potrebbero esser potenzialmente lesi.
  Questo spiega perché, guardando il pensiero di Antonini, l'associazione per delinquere costituisca una deroga al principio di non punibilità degli atti preparatori, definendolo dunque l'art. 416 c.p. come un <<reato di pericolo per una pacifica convivenza sociale>>[51].

Seppur non sempre questo legame tra la nozione di ordine pubblico e la qualificazione del reato di associazione per delinquere come reato di danno o di pericolo rimanga tale in dottrina[52]; in generale bisogna rilevare che, considerato che la maggioranza della dottrina

---

[46]*Ibidem*. Nello stesso senso: De Francesco, (voce) *Associazione per delinquere e associazione di tipo mafioso*, in Digesto delle discipline penalistiche, vol. I, UTET, 1987, pag. 294.
[47]Insolera, *op .cit.,* pag.169.
[48]*Ivi,* pag.170.
[49]*Ibidem.*
[50]Vedi nota 23.
[51]Antonini, *op. cit.,* pag.300.Nello stesso: Fiandaca e Musco, *op. cit.,* pag. 507; pagg.113.
[52]Si cita come esempio Boscarelli, *op. cit*., pagg. 870-871. Egli, nonostante accolga come nozione dell'ordine pubblico il regolare andamento della vita sociale ed il consequenziale senso di tranquillità e sicurezza percepito dai consociati, qualifica il reato di associazione a delinquere come reato di danno. Boscarelli identifica appunto che il pericolo sia un elemento costitutivo della fattispecie, in quanto possa consistere nella commissione di almeno due delitti simili in grado di ledere uno o più interessi penalmente tutelati.
In conclusione, secondo l'Autore:

accoglie la concezione di ordine pubblico in senso materiale, si tende a qualificare l'art. 416 c.p. come reato di pericolo.

Più specificamente, come sostenuto sia da Fiandaca-Musco che dalla Antonini, si tratterebbe di un reato di pericolo concreto: tenuto conto del fatto che il bene protetto è l'ordine pubblico, minacciato dalla semplice esistenza dell'associazione[53], emerge come la *ratio* della norma sia di natura spiccatamente preventiva, perchè solo con l'incriminazione dell'associazione a delinquere in quanto tale il legislatore fa il possibile per eliminare alla radice la possibile commissione dei delitti-scopo[54] .

Antonini, riprendendo la posizione di Insolera sull'ordine pubblico in senso materiale, deduce come <<l'ordine pubblico materiale costituisce l'unica nozione che è possibile ricavare, non certo pienamente, dalla carta costituzionale>>[55], di conseguenza l'art 416 c.p. è una fattispecie di reato di pericolo concreto.

Questo perché la costituzione del sodalizio criminoso, genera infatti una minaccia che è rivolta alla collettività intera poiché i beni messi in pericolo comportano anche la creazione nella popolazione di <<un sentimento di sfiducia nei confronti delle Istituzioni stesse[56]>>. Di conseguenza, la rilevanza penale deve esser esclusa se si può dimostrare che, in quella certa particolare situazione, l'interesse tutelato non abbia corso alcun concreto pericolo[57].

Ma non solo: l'Autrice esclude la qualificazione dell'art 416 c.p. come reato di pericolo astratto: se si accogliesse quest'accezione, si correrebbe il rischio di perdere <<il presupposto di necessaria lesività del bene giuridico tutelato>>quando il bene non corra alcun effettivo pericolo[58], con il conseguente sfumarsi dell'applicazione della sanzione.

A tal proposito, Insolera rileva che la lesione o la messa in pericolo dell'ordine pubblico può sorgere soltanto da comportamenti empiricamente e non da stati meramente soggettivi

---

a) se vi è un lasso di tempo tra la costituzione dell'associazione e l'emergere del pericolo, <<solo a decorrere dal secondo momento la condotta di chi partecipa all'associazione può assumere rilievo di condotta esecutiva del reato>>,
b) la condotta di partecipazione viene meno nel momento in cui cessa il pericolo.

[53]Fiandaca-Musco, *Diritto Penale Parte Speciale, Vol .I,* Zanichelli,2021, pag.507.

[54]*Ibidem.*

[55]Antonini, *op. cit.,* pag. 317.

[56] *Ibidem.*

[57]*Ivi,* pag. 318.

[58]*Ivi.,* pag. 317.

o da atteggiamenti propri della volontà o dell'abito morale dell'agente. È necessaria dunque una riconoscibilità oggettiva della condotta[59].

Sommariamente, anche la prevalente giurisprudenza risulta esser d'accordo nel qualificare l'art.416 come reato di pericolo: si veda, ad esempio, la sentenza della Cassazione penale, sez. VI n. 4294/2014, che ritiene la non configurabilità del tentativo dell'art.416 c.p. se l'organizzazione non risulta essersi ancora costituita, proprio per la natura di reato di pericolo dell'art.416 c.p. .

Considerato che il perfezionamento del reato avverrebbe già solo con la formazione del vincolo associativo e con l'accordo per <<il piano organizzativo per l'attuazione del programma delinquenziale>>[60] - per l'associazione a delinquere semplice non è dunque configurabile il tentativo.

Dopo essersi soffermati sui risvolti che l'ordine pubblico risulterebbe avere in riferimento alla qualificazione del reato di associazione a delinquere, ccorre riportare le riflessioni di Iacoviello sulla questione se sia veramente possibile una nuova riqualificazione dell'ordine pubblico.

Innanzitutto, egli ha considerato che, nel tenere in considerazione sia la nozione psicologica di ordine pubblico che quella di ordine pubblico inteso come un sentimento collettivo di sicurezza, emergono due aspetti fondamentali:

- Il primo è che l'espressione <<ordine pubblico>> denota <<una realtà sociale effettiva[61]>>, ossia un contesto sociale che sia inserito in uno specifico spazio e tempo,
- Il secondo aspetto è come il termine venga utilizzato in connessione a <<fenomeni di vittimizzazione indeterminata, fungibile, […] casuale>>[62].

In seguito, focalizzandosi di più sugli aspetti criminologici e giuridici rispetto a quelli sociologici, egli afferma che l'ordine pubblico sarebbe in realtà <<una grandezza >>[63] le cui dimensioni variano in base alle tipologie degli atti e delle opportunità criminali del sistema presenti in quel momento. Questa grandezza può esser talmente estesa da

[59]Insolera, *op. cit.,* pagg.194-5.
[60]Cassazione penale sez. VI , n. 4294/2014, in *Rivista Penale*, 2015, Vol.3, pag. 244.
[61]Iacoviello, *op. cit.,* pag 51.
[62]*Ibidem.*
[63]*Ivi,* pag.52. Sempre citando l'Autore alla medesima pagina, gli atti criminali corrispondono<<all'intera area di ciò che in un determinato momento è reato>>, mentre le opportunità criminali invece sono <<l'insieme dei fatti e delle situazioni propedeutiche alla commissione dei reati>>.

includere atti e fatti non in grado di costituire pericolo: ecco dunque la nozione di idoneità offensiva, <<criterio che dimensiona [l'area criminogena, N.d.A.] in termini definiti>>[64].

Di fatto, riprendendo la fattispecie dell'associazione per delinquere, Iacoviello definisce che ciò che caratterizza l'associazione a delinquere non è tanto la produzione di reati, ma <<la produzione di opportunità di reati>>[65]: questo perché, proprio per il fatto di essersi posta in essere nella società civile, viene potenzialmente aumentata la capacità di commissione di reati.

Inoltre, il fatto che l'associazione a delinquere possa colpire qualsiasi tipologia di soggetto nella società connota dunque questa fattispecie di reato anche come <<reato a vittima indiscriminata>>[66]. Perciò, Iacoviello qualifica come reato contro l'ordine pubblico <<quel reato a vittima indiscriminata i cui effetti consistono in un aumento statisticamente apprezzabile delle opportunità criminali di un sistema sociale dato>>[67].

Si rileva come il difficile inquadramento del bene giuridico si rifletta anche sulla stessa fattispecie: questo perché, come definito dallo stesso Iacoviello, il bene giuridico contribuisce anche a definire la stessa fattispecie[68].

Infatti, per l'Autore, il rapporto tra tipicità e bene si basa sia sul piano ontologico che epistemologico:

- Riguardo il primo, visto che il bene fonda la tipicità della fattispecie, ne consegue che l'esistenza stessa del fatto comporta il rilevare in concreto e tramite giudizio *ex post* l'offensività della condotta[69],
- Quanto alla determinatezza del bene , il bene giuridico costituisce un <<elemento complementare di conoscenza e determinazione della fattispecie>>[70], grazie ad un giudizio ex ante di idoneità.

Da quest'ultima considerazione, si può concludere come il difficile inquadramento di un bene sfuggente, in costante evoluzione, per la cui definizione bisogna tenere in considerazione contemporaneamente diversi aspetti (da quello psicologico ai principi etici

[64] *Ibidem.*
[65] Iacoviello,*op. cit.,* pag.53
[66] *Ibidem.*
[67] *Ibidem.*
[68] Iacoviello, *op. cit.,* pag.56.
[69] *Ibidem.*
[70] *Ibidem.*

e sociali che reggono una società) come l'ordine pubblico, si riversi automaticamente sull'inquadramento della fattispecie associativa in esame, in particolare sulla mancanza di tipicità.

Quest'ultimo aspetto comporta delle conseguenze problematiche per la disposizione penale in esame, non solo a livello concettuale, ma anche a livello pratico.

Infatti, diventa complesso non solo ogni giudizio di concreta lesività del fatto tipico, ma diventa pure problematica la stessa identificazione della condotta tipica, non descritta, ma piuttosto resa come allusione evocata mediante l'elemento normativo della <<associazione>>, la quale, <<proprio per la sua multiforme fenomenologia, tradisce una fievole capacità di tipizzazione>>[71].

Ma non solo: altra dottrina segnala anche che la mancanza di tipicità della fattispecie incide pure sulla difficoltà di usare la fattispecie come strumento contro una criminalità organizzata in costante mutamento e sviluppo,nonché sul rischio di <<dilatare la portata [della norma]anche oltre quei canoni di garanzia che informano il nostro sistema penale>>[72]. Viste anche queste gravi criticità, si registra uno sforzo (sia della dottrina che della giurisprudenza) nella ricerca dell'elemento oggettivo caratterizzante la fattispecie negli altrettanti elementi connotanti l'art 416 c.p.: in *primis*, l'organizzazione e lo scopo, concetti astratti e suscettibili di diverse interpretazioni (come si vedrà in seguito).

Già da queste problematiche incontrate solo considerando il bene giuridico protetto dalla norma, è corretto segnalare sin dall'inizio della nostra trattazione come non pochi studiosi affermino la necessità di riformulazione dell'intera fattispecie, allo scopo di <<recuperare quella oggettività che nel tempo è andata perduta ed <<offrire quei punti di riferimento concettuale cui di volta in volta, nei singoli casi concreti, la giurisprudenza possa appoggiarsi>>[73]- tenendo sempre in considerazione quali sono state le ragioni che hanno permesso la formazione e l'evoluzione della norma.

[71] *Ivi,* pag.42
[72] Antonini, *op.cit.* pag. 305
[73] *Ibidem.* Si veda anche, sul punto: Grosso, *op. cit.* , pag. 418.

2. La problematicità della nozione di "associazione"

Denotata la difficoltà nel delineare il bene giuridico tutelato dalla norma, occorre procedere al cuore della trattazione di questo capitolo, ossia all'analisi degli elementi costituenti l'associazione,il fatto tipico della fattispecie.

Questa è un'impresa che (come si vedrà) è tutt'altro di immediata risoluzione e che configura diverse posizioni sull'argomento, sia dottrinali che giurisprudenziali. Infatti, come detto correttamente in dottrina<<la legge, tuttavia, non precisa in cosa debba consistere l'associazione e quali ne siano gli elementi costitutivi>>[74].

Un problema centrale è infatti la carenza di tipicità dell'art 416 c.p.: il solo riferimento nell'articolo all'<<associazione di tre o più persone>> e <<lo scopo di commettere più delitti>>[75,] comporta che non venga rispettato il principio di tipicità, tanto che alcuni studiosi si sono seriamente interrogati sulla compatibilità della maggior parte delle fattispecie associative previste dall'ordinamento italiano con il principio di tassatività di cui all'art.25 Cost.[76.]

Un ramo della dottrina precisa come la carenza di tassatività induce ad una lettura della norma incentrata su parametri soggettivi, <<incompatibili con i principi costituzionali di garanzia che governano la struttura dell'illecito penale>> [77] . Ma non solo: questa problematica, risulta esser frutto di una scelta di politica criminale, posta sull'esigenza di dar vita ad una norma estremamente elastica <<per superare il regime di non punibilità degli atti preparatori, ovvero, per assicurare un surplus di coazione processuale. >>[78].

Nonostante la denotata <<genericità>> [79] della norma, dovuta al processo storico di <<smaterializzazione della fattispecie>> [80] , si cercherà in questo capitolo di dare un

[74] Borsari, Provolo, *op. cit*., pag. 34.
[75]Art. 416, Codice Penale.
[76]C. F. Grosso, *op.*, pag.413.
[77] *Ibidem*.
[78] *Ibidem*.
[79]*Ibidem*.
[80] Iacoviello, *op. cit*., pagg. 41- 42. L'Autore, in queste pagine, fa un percorso dettagliato sull'evoluzione storica della normativa: partendo dagli artt. 265 e 266 del Codice Napoleonico del 1810, volti a punire le <<associazioni di malfattori>> ed incentrati sul dato oggettivo dell'organizzazione della banda, fino al passaggio al codice Rocco, dove si è invece scelto di predisporre una fattispecie in cui la norma è tutela un <<bene giuridico impalpabile>> tramite il pericolo presunto: questo, di conseguenza, ha reso per l'Autore <<problematica la stessa identificazione della condotta tipica, evocata più che descritta mediante l'elemento normativo dell'associazione>>.

inquadramento degli elementi necessari per la costituzione di un'associazione criminosa, confrontando i diversi orientamenti della dottrina e della giurisprudenza..

Si procederà, dunque, nell'ordine, nella trattazione de:

a) Il vincolo associativo

b) Il programma criminoso

c) La struttura organizzativa.

2.1. Il vincolo associativo e la sua autonomia dai delitti-scopo.

Dato che ogni associazione è composta da una collettività di soggetti, organizzati in vista del conseguimento di uno scopo comune, è necessario vedere come presupposto la stipulazione di <<un accordo onde ciascuno si assuma di compiere attività […] necessarie al conseguimento dello scopo>>[81].

Come punto di partenza nella trattazione dei tratti essenziali del fatto tipico bisognerebbe perciò partire dall'accordo associativo, in quanto corrisponderebbe alla decisione d'un insieme di soggetti (almeno tre[82]) di porre il proprio contributo per il raggiungimento di uno scopo comune.

Ai fini dell'accertamento dell'accordo associativo, è utile eseguire una distinzione riguardo il momento in cui un soggetto acquisisce la qualifica di associato, a seconda se l'atto di associazione sia o non sia requisito per la costituzione dell'associazione[83]:

1) Nel primo caso, questa situazione si realizzerebbe quando più soggetti manifestano contestualmente la volontà di raggiungere un obiettivo comune. In questa situazione, l'atto di associazione sarebbe anche la stessa manifestazione di volontà dell'individuo partecipante alla convenzione costituente l'associazione;
2) Nel secondo caso si tratterebbe invece quando l'ente associativo è già costituto: qui è sempre necessaria una manifestazione di volontà di adesione dell'individuo ma, a

[81]Boscarelli, voce *Associazione per delinquere* , in Enciclopedia del Diritto, Vol. III , 1958, pag. 865.

[82]Facendo una breve digressione sul numero minimo degli associati, sia la dottrina che la giurisprudenza tendono a valutarlo in termini strettamente oggettivi, ossia <<la componente umana esistente ed effettiva del sodalizio e non gli imputati presenti al processo>> (Cass. pen. sez. VI n. 12845/2005). Per la dottrina, si richiama ~~a~~ : Fiandaca, Musco, *op. cit.,* pag. 508. Per la giurisprudenza: Cass. pen. sez. VI n. 12845/2005, in *Cass. Pen*., 2006 vol.4, pag. 1459; Cass. pen. sez. VI n.17018 del 28/05/2020, in *Redazione Giuffrè* 2020.
Si segnala anche la problematica relativa al considerare o meno anche i soggetti capaci di intendere e di volere, oggetto di pareri contrastanti. In senso affermativo, si cita: Consulich, *op. cit.,* pagg.117-8; Boscarelli, *op. cit.,*pag. 868; *contra:* Cass. pen. 31/3/1952, cit., in *Giust. Pen*., 1952, vol. II, pag. 814.

[83]Boscarelli,voce *Associazione per delinquere* , in *Enciclopedia del Diritto*, Vol. III , 1958, pag. 866.

differenza del caso precedente, questa ha natura integrante rispetto alla convenzione già preesistente.

Nonostante questa breve distinzione, è importante precisare che, ai fini dell'efficacia, l'atto associativo non debba esser necessariamente una manifestazione di volontà espressa[84].

Il mero accordo associativo non è di per sé sufficiente, in quanto, affinché si costituisca l'associazione a delinquere semplice, è stato rilevato nella giurisprudenza [85] l'imprescindibilità di una concreta esplicazione dell'associazione nel mondo esterno affinché possa essa esser considerata penalmente rilevante, non solo da un punto processuale ma in primis da un punto di vista penale.
Quest'ultimo punto è ormai ben consolidato ed anche accolto unanimemente dalla maggioranza della dottrina[86]. Viene infatti definita l'associazione come <<un corpo

[84]Nello stesso senso: Borsari,Provolo, *Associazione per delinquere*, pagg. 31-32. Per la Giurisprudenza: Cass. Pen. Sez. II n. 28868/2020, dove si identifica che la consapevolezza dell'associato <<può esser provata attraverso comportamenti significativi che si concretino in una attiva e stabile partecipazione >>.
Inoltre, facendo un breve riferimento al pensiero di Manzini *Trattato di diritto penale italiano*, (a cura di Nuvolone e Pisapia), UTET ,1981, non risulta esser necessaria la presenza di uno statuto o altro atto costitutivo dell'associazione affinché sussista l'accordo associativo. (Nello stesso senso: Cass., Sez. I, 23 aprile 1985, in *Foro It*., 1986, Vol. II, pag. 595. *Contra*: Boscarelli, *op. cit.,*pagg. 865-6). Questa distinzione di Boscarelli viene approfondita pure da:Tona, *I reati associativi e di contiguità (artt. 416-8),* in *Trattato di Diritto Penale-Parte Speciale, Vol. III*, (a cura di): Cadoppi, Canestrari,Manna, Papa, UTET Giuridica, 2008, pag. 1079, identificando come la stessa natura dell'accordo muti a seconda se l'aspetto associativo si verifica allo stesso momento della nascita dell'ente oppure se invece entri in un momento successivo, ossia quando l'ente ha già una propria struttura. Egli compie un'interessante osservazione sul punto: nella prima ipotesi infatti, non solo identifica come la consumazione del reato sussisterebbe solo al momento de << l'incontro delle volontà dei singoli componenti […] al momento in cui essi costituiscono il vincolo associativo e strutturano il gruppo>>; ma accenna anche a come molto spesso risulta esser problematica la ricostruzione del luogo e del tempo in riferimento alla commissione del reato, poiché risultano mancare molto spesso prove riguardanti il modo ed il momento in cui si è costituita l'associazione.

[85]Si fa riferimento, in particolare, alla questione dell'individuazione della competenza rispetto al reato d'associazione semplice in caso di mancanza di prove sulla nascita del sodalizio. Nello specifico, bisogna fare un breve cenno a tre diversi orientamenti giurisprudenziali:

- Il primo considera la consumazione del reato non al momento della nascita dell'accordo associativo, ma nella fase successiva di programmazione, ideazione e direzione delle attività criminose, ossia nel momento in cui risulti esservi l'effettiva messa in moto delle varie operazioni da parte dell'associazione (Cass. Pen., Sez. II n. 50338/2015 in *Cass. Pen*. , 2016, Vol. 4, pag. 1704; Cass. Pen., Sez. II, n.22953/2012);
- Il secondo invece, vede la consumazione del reato nella commissione del primo tra i reati programmati. In altre parole, assumerebbe rilevanza <<il luogo in cui l'operatività del sodalizio criminoso divenga esternamente percepibile per la prima volta>>(Cass. Pen., Sez. III, n. 24263/2007, in C.E.D. Cassazione 2008. Vedi anche: Cass. pen., Sez. III, n.35578/2016, in C.E.D. Cassazione 2016);
- Un terzo orientamento (minoritario), infine,individua il momento consumativo del reato nella prima manifestazione esterna del vincolo associativo, con la presenza <<degli elementi sintomatici dell'origine dell'associazione nello spazio>> (Cass. Pen Sez. III, n. 35521/2007, in C.E.D. Cassazione n. 237397; Cass. pen., Sez. VI, n.26010/2004, in *Riv. Pen*., 2005, pag. 1391; Cass. pen., Sez. III, n.29899/2011, in*Guida al Diritto* , 2011, n. 45, pag. 84). Per maggiori approfondimenti sul punto, cfr. : Tona, *op. cit.,* pag. 1079.

[86]Tra i numerosi autori a sostegno di quest'affermazione si cita: *Ibidem*; Antonini, *op. cit.,* pag. 306, secondo la quale il mero accordo di tre o più persone comporterebbe piuttosto <<l'applicazione di una misura di sicurezza, secondo quanto disposto dall'art.115 del codice penale>>.

sociale>> [87] , ossia <<un'unità concreta, distinta dagli individui che in essa si comprendono>>[88]: è perciò necessario individuare quali sarebbero gli ulteriori elementi che consentano lo svilupparsi dell'accordo in vincolo associativo(o l'adesione ad esso, qualora fosse già esistente l'associazione a delinquere).

Un ramo della dottrina identifica che il vincolo associativo nasce come diretta conseguenza dell'accordo, ma solo se il vincolo stesso <<traduce l'oggetto di tale accordo e il suo significato criminogeno>>[89]. Affinché ciò avvenga, devono esser perciò presenti questi elementi nell'accordo associativo (si ricorda, sempre stipulato tra almeno tre persone):

1. La presenza di un programma delittuoso (le cui caratteristiche verranno trattate in seguito[90]), avente ad oggetto la commissione di più delitti;
2. L'<<*impegno associativo*>>[91], ossia la solidale condivisione del programma, capace di andare oltre gli accordi volti all'esecuzione dei singoli delitti-scopo;
3. La presenza di un *minimum* di una struttura organizzativa[92] che conferisca un carattere *tendenzialmente permanente*, o comunque stabile[93] al vincolo associativo, destinato a durare oltre la realizzazione dei reati-scopo[94].

Importante segnalare che, riguardo all'ultimo punto, la giurisprudenza[95] rileva due aspetti fondamentali:

- Non risulta necessaria l'assoluta permanenza del vincolo, ma è sufficiente che il vincolo associativo <<non sia a priori e programmaticamente circoscritto a uno o più delitti predeterminati>>[96],

---

[87]Boscarelli, (voce)*Associazione per delinquere* , in Enciclopedia del Diritto, Vol. III , 1958, pag. 865.
[88]*Ibidem.*
[89]Tona,*op. cit.* , pag. 1080.
[90]Si rimanda al punto 2.2. del presente capitolo.
[91] Questa definizione la si ritrova nella sentenza Cass. pen., Sez. I n. 4805/1993, in Cass. pen. fasc. I, 1995, pagg.11-13.
[92]Sul fatto che sia necessario una minima struttura organizzativa idonea a garantire stabilità, si veda: Misaggi, *Associazione per delinquere e concorso di persone nel reato continuato: il confine è davvero sottile?,* nota alla sentenza Cass. Pen., Sez. III, n.11570/2020, in *Diritto Penale E Uomo,* fasc. 9/2020, pag. 891. Quest'aspetto è stato criticato da Iacoviello, *op. cit.,* pag. 43, che, ai fini di dare una caratterizzazione alla fattispecie, identifica come con l'accoglimento di quest'accezione, si ha il rischio che l'elemento dell'organizzazione non acquisisca un'autonomia rispetto ai delitti-scopo, ma piuttosto rimanga <<un'attività essenzialmente propedeutica e strumentale alla realizzazione di tali delitti>>.
[93]Per la stabilità del vincolo come sufficiente elemento alla sua configurazione, si veda: Cass. pen. Sez. I del 03/10/1989, in *Giust. Pen*. 1990, vol. II, pag. 610; Cass. pen. Sez. V, n. 12525/2000, in *Cass. pen*. 2001, Vol.10, p.2686; Cass. pen. Sez. I n. 39757 del 28/09/2005, in *Giur. It*., fasc.7/2006, pag. 1483.
[94]Cfr.: Cass. pen., Sez. VI, 27/05/1991, cit., in *Giur. It*., 1993, vol. II, pag. 163,secondo cui non è necessaria la presenza di un patto espresso fra gli associati, essendo sufficiente piuttosto che essi siano in grado di agire anche in assenza di un accordo, ma <<nella consapevolezza che le attività proprie ed altrui ricevono vicendevole ausilio e che insieme contribuiscono ad attuare il programma delle attività criminali».
[95]Cass. pen. sez. V n. 12525/2000, in Cass. pen. 2001, pag.2685.
[96] Nello stesso senso Tona, *op. cit.,*pag.1080. Sulla base di questa sentenza, Consulich, *op. cit.*, pag.115, qualifica il reato di associazione a delinquere semplice come <<reato permanente>>. Sulla natura permanente

- L'elemento temporale, riferito alla nozione stessa di stabilità del vincolo associativo, non va necessariamente inteso come necessario protrarsi del legame criminale: basta, ai fini della sussistenza dell'elemento materiale del reato, <<una partecipazione all'associazione anche limitata ad un breve periodo>>[97].

Riassumendo, solo con la presenza di questi quattro elementi caratterizzanti il vincolo associativo (il quarto, si ricorda, si ritrova nella manifestazione della volontà di almeno tre persone di porre in essere l'associazione o di aderirvi ad essa); si garantisce la creazione di una struttura concreta, in grado di perseguire il programma delittuoso condiviso dai partecipanti fino alla sua piena realizzazione, manifestando all'esterno la sua portata criminale.

La vera essenza del vincolo associativo è dunque il suo essere in grado di seguire un programma criminoso e capace di manifestare nel mondo esterno la sua portata proiettandosi oltre la realizzazione del delitto o del gruppo di delitti (riassumibile perfettamente come la <<capacità a perdurare>>[98]). Questo stesso elemento è anche un elemento chiave per non solo esplorare più approfonditamente la ratio incriminatrice dell'art. 416 c.p, ma anche per ricavare un importante corollario da tenere in considerazione nella disamina del vincolo associativo: la distinzione tra la responsabilità penale dell'associazione rispetto a quella relativa ai delitti-scopo commessi.

Per comprendere meglio la questione, bisogna riprendere con attenzione il primo comma della norma 416 c.p.: <<*Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni*>>.

---

del reato fa un'interessante osservazione De Francesco, (voce) *Associazione per delinquere e associazione di tipo mafioso,* in Digesto disc.pen., I, Torino, 1987; che identifica chiaramente a pag. 291come in realtà non sempre la protrazione della condotta esecutiva realizzi necessariamente la permanenza del reato: infatti, seppur <<non può negarsi che, perché l'associazione risulti effettivamente costituita […] debba trascorrere un periodo di tempo apprezzabile>>, questo periodo non può esser computato ai fini di considerare la permanenza del reato: eventualmente, può solo esser considerato il tempo <<dopo che l'associazione si sia effettivamente costituita>>.

[97] Nello stesso senso: Cass. pen. Sez. I del 03/10/1989, in *Cass. pen*. 1991, vol. I , pag.744; dove viene indicato che <<l'elemento temporale non deve essere considerato come notevole protrarsi del rapporto nel tempo, essendo anche sufficiente uno svolgersi dell'attività associativa per breve periodo>>.

[98] De Francesco, *op. cit*.,pag. 291, definisce la <<capacità a perdurare>> come la capacità di proiettarsi oltre la realizzazione del delitto o del gruppo di delitti.

Affinché l'associazione emerga come entità diversa e separata dalle singole condotte criminose, deve esservi una struttura idonea a poter esser nuovamente utilizzata per la commissione di singoli delitti.
Non soffermandosi sul requisito organizzativo (che si tratterà successivamente[99]), per il momento si fa cogliere solo nel caso dell'associazione a delinquere semplice il soggetto avrebbe da svolgere un determinato compito per l'attuazione di un programma criminoso di carattere molto più ampio e generico. [100] .

Questa precisazione permette la trattazione d'un aspetto molto importante: la distinzione tra il vincolo associativo e l'accordo per commettere uno o più reati ex art. 115 c.p.[101] Vi è già un ramo della dottrina[102] concorde sul pensiero che l'accordo diretto a commettere uno o più delitti determinati rimane privo di ogni rilevanza penale, a prescindere se il delitto sia stato commesso o meno: questo perché, una volta commesso il reato-scopo, queste condotte esauriscono il loro compito, in quanto attività puramente preparatorie dello stesso.

Si deve però considerare che il ruolo di questa tipologia di accordi assumerebbe una rilevanza penale non ex-ante (cioè come effettiva preparazione di un reato non ancora commesso), ma si tratterebbe piuttosto d'una rilevanza penale ex-post: ciò che interessa eventualmente è soltanto la loro rilevanza causale per l'accordo stesso[103]. Sulla base di queste considerazioni, si potrebbe immediatamente arrivare a pensare che anche l'associazione abbia un carattere preparatorio rispetto ai singoli delitti-scopo. Invece, la visione predominante della dottrina[104] risulta essere tutt'altra: riportando all'attenzione la

[99] Si richiama alla trattazione del punto 2.3 di questo paragrafo.
[100] Viene riportato l'esempio di: De Francesco, *op. cit*., pagg. 291-292: c'è una chiara differenza tra un gruppo di persone che decidono insieme di commettere un reato di atti persecutori ex art. 612 bis c.p. (più comunemente conosciuto come reato di stalking) e un'associazione per delinquere costituita a scopo di commettere reati persecutori: a differenza della prima situazione, anche nella seconda vi saranno comunque persone che avranno diversi ruoli da svolgere (ad es., il reperire informazioni sulle vittime, il chiamarle persistentemente o mandare messaggi persecutori, il pedinarle costantemente nelle loro attività quotidiane ecc.), ma non allo scopo di commettere un singolo reato persecutorio o quel certo gruppo di reati persecutori, piuttosto allo scopo di commettere *il reato di atti persecutori* o *una serie di reati di atti persecutori*. *Contra:* Cass. pen., Sez. I, 01/07/1988 in Giust. Pen. 1989;
[101] Recuperando brevemente quest'ultima fattispecie, l'art. 115 c.p. esclude ogni forma di responsabilità penale in caso di semplice accordo allo scopo di commettere un reato, laddove questo non sia commesso. In maniera residuale, potrà essere applicata soltanto una misura di sicurezza. La medesima sanzione sostitutiva verrà applicata se v'è stata l'istigazione, ma il reato incitato non è stato commesso.
[102] Patalano, *op. cit*., pag.43.
[103] De Francesco, *op.cit.,* pag. 294.
[104] Si fa riferimento a: Consulich, *Reati contro l'ordine pubblico*, in Antolisei (agg. a cura di Grosso), *Manuale di diritto penale. Parte speciale*, vol. II, Giuffré, 1968, pag.715. Arriva alla stessa conclusione anche: Del Corso, *I nebulosi confini tra associazione per delinquere e concorso di persone nel reato continuato*, in *Cass. Pen*., 1985, vol.4, pag. 626.

lettura della fattispecie, il <<per ciò solo>> [105] , indicherebbe chiaramente che l'associazione debba considerarsi illecita e punibile come reato a sé stante,a prescindere o meno dal fatto che siano stati o non stati posti concretamente atti delittuosi[106].

Di conseguenza, la caratteristica dell'indeterminatezza del programma criminoso[107] (cioè il procedere per la commissione della tipologia del <<tipo astratto di reato attraverso una pluralità indeterminata di fatti criminosi>>[108]) indicata all'articolo 416 determinerebbe:

- L'autonomia della condotta associativa rispetto alle attività di partecipazione dei singoli delitti-scopo [109] : a differenza del mero accordo, se la persona non esplica l'attività corrispondente alla sua competenza o funzione ovvero non partecipa completamente alla commissione di uno o più reati, rimane comunque rilevante la sua condotta associativa, proprio per la <<permanenza come ruolo potenzialmente utilizzabile>>[110]per la potenziale realizzazione di ulteriori reati.

  Da questo, ne consegue che il soggetto sarà comunque ritenuto, su piani diversi, responsabile penalmente sia ex art. 416 c.p., sia per i reati-scopo a cui abbia fornito un contributo casuale (sempre se, chiaramente, abbia partecipato alla loro realizzazione).
- L'autonomia sul piano soggettivo: il fatto che gli associati si rivolgano ad un progetto indeterminato di reati comporta, a differenza dell'art.115 c.p., la necessaria presenza dell'intenzione di costituirsi in ruoli e competenze predeterminate rispetto alla commissione dei singoli reati, <<pensati dunque come elementi strutturali permanenti del vincolo associativo>>[111].

---

[105] Art.416[1], Codice Penale.

[106]Questo permette un collegamento alla ratio incriminatrice della norma, espressa da : Consulich, *Reati contro l'ordine pubblico*, in Antolisei (agg. a cura di Grosso), *Manuale di diritto penale. Parte speciale*, vol. II, Giuffré, 2016, pag. 113: <<l'esistenza di una associazione per delinquere costituisce un fenomeno antagonistico per l'ordinamento e alla sua scala di valori,quindi, di per sé sola, e cioè, indipendentemente dai delitti che siano stati commessi, determina una condizione disvoluta dal sistema penale>>. Si cita anche la visione di: Aleo,*op. cit.,* pag. 36, che identifica come le figure delittuose associative abbiano avuto una anticipazione della soglia della risposta e responsabilità penale, <<in considerazione della particolare entità dell'oggetto della tutela e del pericolo>>.

[107]De Francesco, *op. cit.,* pag. 298., sembrerebbe esser d'accordo su questi ragionamenti posti dalla dottrina prevalente, se non per una non marginale differenza: non è la caratteristica dell'indeterminatezza del programma a creare questi importanti sviluppi summenzionati, quanto piuttosto la natura potenzialmente permanente della struttura organizzativa: il fatto che le funzioni o competenze associative abbiano un carattere indipendente rispetto a delle attività preparatorie delittuose (che di volta in volta ne integreranno il contenuto), rende i singoli ruoli in grado di perdurare oltre la specifica fase del delitto concordato. Cfr. anche: Aleo, *op.cit.,* pagg.42-3.

[108]De Francesco, *op. cit.,* ,pag. 290.

[109]Si veda: Cass. pen. Sez. II, n.36251/2020, in C.E.D. Cass. Pen. 2021; Cass. pen., Sez. I, 14/11/1980, in *Giust. Pen*., 1981; Cass. pen., Sez. I, 01/07/1988 in *Giust. pen*., 1989.

[110] De Francesco, *op. cit.*, 291.

[111]*Ibidem*. Si segnala però la presenza di sentenze che negano la necessaria presenza di gerarchie interne e distribuzione di cariche, essendo sufficiente l'esistenza di un vincolo non circoscritto a determinati delitti ma

- Infine, questa capacità a perdurare[112] dell'associazione, permette chiaramente di percepire che l'art. 416 c.p. sia una deroga alla non punibilità dell'accordo a commettere più reati ex art.115 c.p.: questo perché la fattispecie deve esser valutata non in base al rapporto ai singoli episodi del piano delittuoso, bensì <<[...] in relazione del suo carattere di fattispecie permanente, costituita da un insieme di funzioni stabili in vista di un progetto criminoso indeterminato>>[113].

In conclusione, il ramo maggioritario della dottrina vede nell' l'articolo 416 c.p. la giustificazione come deroga all'art. 115 c.p. <<per l'autonomo significato lesivo dell'ordine pubblico>>[114], in quanto ente autonomo con una propria struttura volta all'obiettivo di raggiungere il compimento del programma criminoso.[115]

Bisogna però riportare un'interessante critica sul punto, posta al fine di capire se l'accordo sia un elemento sufficiente per consentire la qualificazione della fattispecie dell'associazione a delinquere come autonoma, eseguendo un confronto con l'articolo 115 c.p.[116] ed altre due fattispecie rientranti nella deroga dell'art. 115 c.p., ossia i fenomeni dell'istigazione e dell'apologia a delinquere ex art 414 c.p.[117] . Visto che la caratteristica dell'istigazione a delinquere tale da rendere autonoma la fattispecie dall'art.115 c.p risulta

---

esteso ad un generico programma: Cass. pen., Sez. VI, n.468/1998, in *Rass. Avv. Stato*, 1999; Cass. pen., Sez. I, 01/07/1988, in *Gius. Pen*.,1989.

[112]*Contra:* Tona, *op.cit.,* pag. 1066; Iacoviello, *op. cit*., pag. 60, che ricollegano l'elemento distintivo tra l'articolo 416 c.p. e l'art.115 c.p. all'elemento organizzativo. Infine, si cita anche la sentenza Cass. pen. sez. V n. 25251/2021, in *Redazione Giuffrè* 2021, che invece ricollega la distinzione all'indeterminatezza del programma criminoso.

[113]De Francesco, *op. cit.*, pag. 294.

[114]*Ibidem.*

[115]Consulich*, op. cit.*, pag.113.

[116]Insolera, *op. cit*., pag. 74 e ss., riprende alcuni orientamenti dottrinali a sostegno della qualificazione dell'art.416 c.p. come deroga al regime di non punibilità dell'accordo per commettere più reati:

- Chi sostiene che l'accordo criminoso si distingue come deroga in quanto elemento distintivo rispetto all'istigazione o all'accordo posto per commettere più reati (si cita: Santoro, *Manuale di Diritto Penale,* I, UTET, 1958,pag.513);
- Chi invece fa sostegno sull'argomentazione che l'accordo tra le parti sia elemento sufficiente per la configurazione della fattispecie, senza bisogno di ulteriori elementi oggettivi (si cita, sul punto: Grispigni, *Diritto Penale Italiano,* Vol.II, Giuffrè, 1947, pag.233). Questo pensiero viene poi specificato ulteriormente da: Misaggi, *Associazione per delinquere e concorso di persone nel reato continuato: il confine è davvero sottile*?, nota alla sentenza Cass. Pen. Sez. III, n.11570/2020, in *Diritto Penale E Uomo*, fascicolo 9/2020, a pag.88; in cui specifica che queste posizioni si basavano sugli artt. 304 e 305 c.p., nei quali si distingueva (e differentemente, si puniva) la cospirazione politica mediante accordo e la cospirazione. Per Insolera, *op. cit*., pag. 78, nessuna delle due teorie sovracitate conferisce autonomia alla fattispecie.

[117]Riprendendo velocemente le figure di reato summenzionate:

- L'istigazione a delinquere, ex art. 414 c.p.,corrisponderebbe alla sollecitazione pubblica alla commissione di uno o più reati;
- L'apologia di reato, indicata nell'art 414^3 c.p., si differenzia dall'istigazione non solo per il fatto che può riguardare solo la commissione di delitti e non contravvenzioni, ma anche perché consiste <<nella rievocazione pubblica di un episodio criminoso diretta e idonea a provocare la violazione delle norme penali>>. (Cass. pen. Sez. I, n. 40552/2009).

essere la pubblicità nella modalità di condotta dell'autore del reato[118], se si confronta l'istigazione con l'accordo dell'art.416 c.p., si noteràcome in quest'ultima norma si rimandi immediatamente alla nozione di associazione, e non siano presenti altri requisiti relativi all'accordo tra i partecipanti [119] : questo perciò non solo comporta che la disposizione della norma contrasti con le disposizioni dell'art.414 c.p. e come non sia possibile individuare il requisito della pubblicità degli atti, ma anche emerge che manca <<l'esplicito riferimento a particolari modalità di condotta idonee a specializzare il tipo di accordo previsto nell'art.416 c.p.>>[120].

Da questo emergerebbe la poca chiarezza anche dello stesso requisito dell' accordo aggrava non poco la problematica d'astrattezza del fatto tipico, la cui determinazione particolarmente necessaria <<laddove il pericolo si collochi all'esterno della fattispecie, come ratio dell'incriminazione>>[121].

Una risposta la perché di questa problematica si può cogliere facendo un confronto con la nozione di associazione presente nell'art.18 Cost.[122]: da esso, si nota che la nozione di associazione indicata all'art.416 è perfettamente congrua al limite intrinseco della libertà di associazione[123] . Ciò denota una scarsa sensibilità del legislatore nella descrizione della fattispecie, poiché, oltre al carattere della finalità a delinquere, rimane solo <<il dato materiale <<neutro>> dell'esistenza del sodalizio>> [124] , mancando dunque ulteriori elementi che arricchiscano la fattispecie e che allo stesso tempo rendano più evidente le polarità tra i due articoli.

È infatti avvenuto, sia in dottrina che in giurisprudenza un lento spostamento dell'attenzione <<dal polo materiale>>[125], dato dal dato del sodalizio organizzato, alla dimensione finalistica intrinsecamente illecita, arrivando a configurare l'associazione per

---

[118]Secondo Insolera, *op. cit.*, pag.81, <<quella modalità dell'azione è significativa di una sua idoneità a porre in essere il bene giuridico tutelato>>. Egli , inoltre, accenna nella stessa pag., che sulla base della pubblicità delle azioni istigatorie si è sviluppata una cospicua giurisprudenza sostenente la teorica dei reati di pericolo presunto per l'ordine pubblico, nonostante egli non risulti esser d'accordo sul punto (su questo, si rimanda al paragrafo precedente, riguardante la trattazione del bene giuridico).

[119]*Ivi,* pag. 83.

[120]*Ibidem.*

[121]*Ibidem.*

[122]<<I cittadini che hanno diritto di associarsi liberamente, senza autorizzazione, per fini che non sono vietati ai singoli dalla legge penale. Sono proibite le associazioni segrete e quelle che perseguono, anche indirettamente, scopi politici mediante organizzazioni di carattere militare>>.

[123]De Vero, *I reati associativi nell'odierno sistema penale*, in *I reati associativi,* Ministero di grazia e giustizia, & Fondazione Centro internazionale su diritto società ed economia., 1998,Giuffrè; spiega a pag. 19 che questo limite altro non è se non <<l'illiceità penale dei fini perseguiti e peculiarità organizzative e/o progettuali come fondamento di particolari divieti di associarsi, pur in vista di programmi non intrinsecamente criminosi>>.

[124]*Ivi,* pag.20.

[125]*Ivi,* pag.21.

delinquere come una forma di <<accordo criminoso qualificato>>[126]. Questo quadro generale ha avuto origine da due fattori:

- La scelta, presente già dai codici preunitari, di porre l'anticipazione della tutela[127] rispetto ai reati contro l'ordine pubblico aggredito dai delitti-scopo, ha portato alla progressiva dispersione degli elementi caratterizzanti la fattispecie associativa;
- Una scarsa <<visibilità>> a livello sociale delle associazioni a delinquere,che (prima dell'emergenza della criminalità organizzata) ha provocato ben poco interesse al legislatore nell'indagare meglio il disvalore penale presente nello stesso concetto d'associazione nei fenomeni di associazione criminosa.

Solo in tempi più recenti la dottrina ha mostrato uno sforzo maggiore nello svincolare l'aspetto strutturale ed organizzativo dalle problematiche inerenti sia l'accordo criminoso sia la punibilità degli atti preparatori dei delitti-scopo.

Considerato che la vera essenza dell'associazione risulterebbe essere un'organizzazione stabile, capace di creare <<una vera e propria <<macchina>>criminosa >>[128] ed in grado di richiamare a sé potenziali intenti illeciti[129], s'incoraggia gli studiosi e la giurisprudenza a focalizzarsi di più sull'elemento organizzativo: in questo modo non solo si assicurerà la determinatezza della fattispecie, ma anche si consentirà allo stesso fine delittuoso di assumere << una […] proiezione dinamica della struttura organizzata>>[130].

Da questa disamina di questo primo elemento del fatto tipico della fattispecie associativa, è chiaro come già al primo impatto si presentano non poche insidie: se da un lato, dottrina e giurisprudenza hanno raggiunto una condivisione piuttosto solida nella individuazione degli elementi costitutivi del vincolo associativo (seppur talvolta con qualche parere contrastante sulle caratteristiche di questi ultimi); davanti invece alla problematica della configurazione dell'art.416 c.p. come deroga all'accordo di commettere uno o più reati ex art.115 c.p. .

In realtà, nonostante la superficiale concordia, emergono tra i giuristi non pochi dubbi e pareri contrastanti, legati sempre alla tematica del vincolo associativo .

---

[126]*Ibidem.*

[127]Questo a conferma di quanto detto finora dell'associazione a delinquere come deroga all'art.115 c.p. .

[128]De Vero, *op. cit.,* pag. 22.

[129]Si veda, in particolare: De Francesco, *Societas sceleris, Tecniche repressive delle associazioni criminali*,in *Riv. It.dir, e Proc.Pen.*, 1992, vol. I, pagg.105-7.

[130]De Vero, *op. cit.,* pag. 22.

Tuttavia, bisogna segnalare come, nella stesura di questo paragrafo, sia emersa molto spesso una vera e propria simbiosi tra il concetto di vincolo associativo e l'elemento dell'apparato organizzativo: aspetto indubbiamente corretto, considerate sia le caratteristiche del vincolo associativo che la tipologia della fattispecie penale in questione, ma che ha portato forse ad uno sovrastare del secondo rispetto al primo, rischiando di far cadere nell'oblio la ricerca di una definizione precisa e chiara per il vincolo associativo.
E, considerando l'emersione sempre più frequente di diverse tipologie di associazioni a delinquere e la necessità di comprendere quali elementi di prova siano necessari per dimostrare l'esistenza del vincolo associativo in sede processuale, si rende ancora più evidente perché questo aspetto richieda un intervento da parte del Legislatore.

2.2. L'indeterminatezza del programma delittuoso.

Oltre all'aspetto del vincolo associativo, non si può considerare la creazione di un'associazione per delinquere senza la presenza di uno scopo perseguito, uno scopo comune agli associati che abbia ad oggetto la commissione di più delitti (non contravvenzioni[131]), avente cioè ad oggetto la realizzazione di un programma delittuoso, caratterizzato dall'indeterminatezza, precedente rispetto agli accordi particolari relativi ai singoli delitti e avente la capacità di sopravvivere agli stessi per l'ulteriore realizzazione del programma stesso[132].
Inoltre, l'indeterminatezza non necessariamente deve riferirsi alla tipologia di delitti, ma può fare riferimento anche al loro numero[133].
Tuttavia, si cercherà di osservare in questo paragrafo cosa comporta la caratterizzazione di questo programma come indeterminato, sia da parte della dottrina che dalla giurisprudenza.

Prima di questa tappa, bisogna però chiarire il concetto dello scopo di commettere più delitti: considerando che il turbamento dell'ordine pubblico si misura anche <<dal numero d'interessi penalmente tutelati che verrebbero ad esser lesi dall'attuazione dello scopo>>[134], lo scopo di commettere più delitti non può non mirare alla realizzazione di

[131] Consulich, *op. cit.,* pag.115.
[132]La definizione si ritrova in: Borsari, Provolo, *op. cit.*, pag. 36.
[133] Fiandaca- Musco, *op.cit.,*pag.115. Nello stesso senso: Cass. pen., Sez. I, n. 66/1997, Ciampà, in *Cass.. Pen*., 1998.
[134]Boscarelli, *op. c*it., pag. 869.

<<singole offese di più interessi penalmente tutelati, o più offese di un unico interesse >>[135].

Più in dettaglio, lo scopo comune dovrà avere ad oggetto (anche non in via esclusiva[136]), alternativamente:

i. La commissione di due delitti il cui oggetto giuridico non si identifichi con un interesse dello Stato e di cui i soggetti passivi non siano persone specificamente individuate (o comunque , siano persone individuate in una stretta cerchia esclusiva) [137];
ii. La commissione di più delitti volti a colpire come bene giuridico, un interesse dello Stato, la cui offesa <<si traduca in pregiudizio di ciascun consociato, in quanto membro della comunità statuale>>[138];
iii. La commissione di più delitti che comporti l'offesa sia d'un interesse dello Stato, ma anche d'un interesse di una persona diversa dallo Stato (i c.d. delitti << a duplice soggetto passivo>>[139] : es. la falsa testimonianza).

È importante precisare che non è richiesta la commissione di una tipologia specifica di delitti[140], così come è irrilevante se i delitti commessi siano tutti dello stesso tipo o no.
Quello che, invece, fa escludere l'applicazione dell'art. 416 è se lo scopo sia la commissione di un singolo reato, ovvero se lo scopo di carattere sia <<genericamente immorale>[141], proprio perché è richiesta chiaramente dalla norma la commissione di più delitti, quindi <<la realizzazione di determinate fattispecie criminose>>[142].

Ma non solo: visto che è proprio lo scopo di commettere più delitti ad essere lo strumento con il quale è possibile distinguere l'associazione a delinquere e la riunione di più soggetti[143], lo scopo comune <<conferisce unità ideale al corpo sociale>>[144].

---

[135]*Ibidem.*
[136]*Ibidem*. Si indica, nella stessa pag., la possibilità che i delitti rientrino in parte in una e in un'altra categoria di quelle che si andranno ad elencare a breve.
[137]Su quest'ultimo aspetto, cfr. Cass. pen. 15/07/1949, cit., in *Giust. pen*., 1949, vol. II, pag.895. Sullo stesso punto sembrerebbe esser concorde Iacoviello, *op. cit.,*pag. 57 , il quale definisce che <<il programma può ben contenere l'ideazione di reati concreti a vittima determinata>>.
[138]*Ibidem*. L'Autore, porta, come es. : spionaggio politico o militare.
[139]*Ibidem.*
[140]Consulich, *op.cit.,* pag.116, arriva a queste conclusioni facendo un breve confronto storico con il reato di associazione indicato nel codice Zanardelli (art. 248).
[141]*Ibidem*. Nello stesso senso, si veda: Fiandaca, Musco, *op. cit.,*pag. 511.
[142]*Ibidem.*
[143]Palazzo, in *Associazioni illecite ed illeciti delle associazioni ,*in *Riv. It. dir. e Proc. Pen*., 1976, pag.418., precisa che, mentre nella riunione è predominante <<il dato materiale della compresenza di più persone in

Tuttavia, la nozione di scopo comune non è unitaria, anzi: oltre alla nozione di scopo comune di commettere più delitti come elemento necessario e presupposto dell'associazione, volta a cementare il concetto di <<societas>>>>>[145]. si deve notare come molto spesso viene travisato con la nozione di scopo <<di natura eminentemente psicologica ed individuale>>, idoneo alla fondazione del concetto di dolo[146], creante il problema del<<duplice operare della nozione dello scopo>>[147] di commettere delitti, sia sul piano oggettivo che sul piano soggettivo.

Trattata la tematica del concetto di scopo, bisogna concentrarsi sul concetto di indeterminatezza del programma delittuoso.
La particolarità dell'indeterminatezza del programma è racchiusa perfettamente in <<ciò che in esso è necessario>> [148] : il programma, oltre alla rappresentazione concreta d'eventuali delitti, deve avere in sé anche la previsione in astratto di specifiche tipologie di delitto attualmente reiterabili.

Questo permette di definire le tre caratteristiche principali di un programma criminoso:

1. <<specificità dei tipi di delitto>>,
2. <<ricorsività dei fatti di reato>>,
3. <<aspecificità delle vittime>>.[149]

La questione dell'indeterminatezza del programma non si dirigerebbe tanto sui delitti, ma piuttosto sui fatti di reato. Infatti, un ramo della dottrina definisce il programma come

---

un determinato ambito spaziale>>, nell'associazione a delinquere predomina un <<dato ideale, e alle volte, precisamente ideologico>.
[144]Insolera, *op. cit.,* pag. 102.
[145]*Ivi*,pag. 103.
[146]Si utilizza la definizione di dolo specifico di: Bricola, *Considerazioni esegetiche sul dolo specifico del reato di falso in scrittura privata,*in *Arch. Pen.*, 1960, vol. II, pag.65, come <<intenzione rivolta al conseguimento d'un evento la cui realizzazione è posta oltre la consumazione formale del reato e rappresenta la consumazione sostanziale di esso>>.
[147]Insolera,*op. cit.,* pag. 104.
[148]Iacoviello, *op. cit.,* pag. 57.
[149]*Ibidem.* Tuttavia, riguardo al punto 3), si richiama alla nota 137, in cui si afferma come l'Autore non escluda la possibilità che alcuni reati rientranti nel programma possano avere vittime predeterminate. Egli sembrerebbe comunque preponderare per l'indiscriminatezza delle vittime dei delitti-scopo, considerando, nella stessa pag., che: <<l'associazione per delinquere è definita dalla sua proprietà di produrre opportunità criminali a vittima indiscriminata […] >>, definendo dunque il programma delittuoso come <<a vittima fungibile>>.

<<una serie di tipologie delittuose, ognuna delle quali è integrata da una serie aperta di eventi (cioè i fatti di reato)>>[150].

Giusto per fare un breve esempio per comprendere quest'ultimo passaggio: dovrebbe esser indicato non tanto nel programma che si intende commettere il reato di truffa e di riciclaggio piuttosto che il traffico d'armi ed il traffico di stupefacenti, ma piuttosto sarebbe sufficiente indicare il bene giuridico che si intende offendere (es. reati contro la persona, reati contro il patrimonio, ecc.), e che siano poste in essere delle condotte di carattere omogeneo.

Con questa precisazione, si può fare una chiara distinzione nei concetti di idoneità ed univocità:

- L'idoneità riguarda il fatto di reato, legato intrinsecamente all'<<adeguatezza causale dell'associazione rispetto al programma>>[151];
- L'univocità concerne piuttosto <<la relazione tra condotta ed intenzionalità>>[152].

Questa distinzione è importante da fare per un motivo: solo la prima caratteristica è intrinsecamente legata al programma[153].

Tirando le somme sul legame tra idoneità e programma[154] si delinea anche tra il programma associativo e la struttura organizzativa, in base ai ragionamenti svolti si possono ricavare due punti fermi:

- la specificità del programma è legata al giudizio di idoneità della struttura organizzativa: se l'associazione a delinquere vuole commettere una serie di reati contro un determinato bene giuridico, dovrà avere un'organizzazione che le consenta di agire secondo i suoi obiettivi[155].
- L'idoneità della struttura è il limite del programma: rileveranno penalmente solo i delitti-scopo che sono realizzabili dall'associazione in base alla sua struttura, <<non anche quelli meramente vagheggiati>>[156].

---

[150] *Ibidem.*

[151] Iacoviello, *op. cit.,* pag. 58.

[152] *Ibidem.*

[153] *Ibidem*. Questo perché, come spiegato nella stessa pag., mentre l'idoneità è logicamente collegata alla fattispecie (oltre ad essere espressamente menzionata); l'univocità <<esprimendo l'autoevidenza del fine della condotta, implica una relazione tra termini definiti>>: cosa che non può riguardare il programma, caratterizzato dall'indeterminatezza stessa. (spostato in nota)

[154] Per maggiori approfondimenti sul rapporto tra idoneità e indeterminatezza del programma delittuoso, si veda: Aleo, *op. cit.,* pagg.153-154.

[155] Es: se l'associazione a delinquere ha come programma associativo la commissione di reati contro il patrimonio, non può avere una struttura idonea alla commissione di reati contro la persona

[156] *Ibidem.*

Data una spiegazione più ampia della nozione d'indeterminatezza del programma, bisogna ora vedere le visioni della giurisprudenza sul punto. Non vi sono mai stati da parte di essa tanti dubbi sull'essenzialità dell'indeterminatezza del programma delittuoso, ma negli anni si sono piuttosto sviluppati due approcci diversi su quest'elemento:

- Alcuni orientamenti hanno fatto leva sull'indeterminatezza del programma criminoso per la distinzione dal concorso di reati, sostenendo come l'indeterminatezza sia un elemento indispensabile per la fattispecie dell'art. 416 c.p.[157];

- Un altro orientamento (che pare stia prendendo sempre più piede) identifica che non è elemento indispensabile la genericità del programma: infatti, la lettera dell'articolo 416 c.p. indica solo la commissione di più delitti, non anche l'indeterminatezza. Secondo un orientamento della Cassazione, infatti, il cuore della norma è quello di <<da un lato, […] assicurare la punizione di condotte che, per un verso, non raggiungono il livello di concorso di persone nel reato>>, dall'altro verso << costituiscono un pericolo per l'ordine pubblico, poiché […] implicano anche l'organizzazione e la predisposizione di mezzi per l'attuazione del programma criminoso>>[158].

In chiusura, un piccolo approfondimento può esser svolto sulla distinzione tra le nozioni d'indeterminatezza del programma e del medesimo disegno criminoso (quest'ultimo presente rispettivamente nel concorso di persone nel reato continuato ex art.81^2 c.p.[159]); nonché - sempre se vi sia davvero una differenza- capire se essa possa essere un elemento sufficiente per distinguere il reato continuato[160] dall'associazione per delinquere. Questa

[157]Cass. pen. del 14/6/1995, cit., in *Cass. pen*., Vol. III,1997, pag. 398. Si veda anche: Corte d'appello - Ancona, n. 719/2021, in *Redazione Giuffrè* 2021. Altre sentenze fanno invece riferimento sia al vincolo associativo che all'indeterminatezza del programma: Cass. pen. del 26/11/198, Trimboli, in *Riv. Pen*., 1989; Cass. pen. sez. V, n. 1964/2018, in C.E.D. Cass. Pen.2019.

[158]Cass. pen. del 30/1/1997, cit., in *Cass. Pen*., 1998, pag. 803. Nello stesso senso, si ritrova il già citato Boscarelli, *op. cit.,* pag. 869. Per la giurisprudenza, si veda anche: Cass. Pen. sez. I n. 67/1997, in *Cass. Pen*., 1998, pag. 803; Cass. pen, Sez. I, n. 66 /1997, Ciampà, in *Cass. Pen*., 1998.

[159] Si riporta qui il testo della fattispecie: <<Alla stessa pena [ossia, la pena più grave aumentata fino al triplo ex art. 81^1, N.d.A.] soggiace chi, con più azioni od omissioni,esecutive di un medesimo disegno criminoso, commette anche in tempi diversi più violazioni della stessa o di diverse disposizioni di legge.>>. La pena viene comunque commisurata nel rispetto del limite dell'art. 81^3 c.p., senza cioè travalicare il tetto della somma materiale delle pene.

[160]Per maggiori riferimenti al reato continuato v.: Misaggi, *ibidem*, pag. 90. Per l'autrice, l'art 81^2 c.p., altro non sarebbe se non <<un concorso materiale arricchito dal medesimo disegno criminoso>>, espressione della <<benevolenza sanzionatoria del Legislatore post-fascista>>, che sceglie in questa tipologia di concorso di non prevedere l'immediata applicazione del criterio <<*tot crimina, tot poenae*>>.Perciò, <<il medesimo disegno criminoso>>, perno della disciplina del reato continuato, determina per l'Autrice che tutti i singoli reati siano stati commessi <<per uno scopo comune, prefissato e specifico>> (*Id*., pag. 91).

questione non è di carattere trascurabile: è stata definita come <<una delle più tormentate questioni attinenti all'illecito associativo>>[161], e tutt'ora è oggetto di discussione.
Da come poi si risponderà a queste problematiche (in particolare alla seconda), si permetterà di dimostrare se l'orientamento giurisprudenziale che ritiene come non indispensabile l'indeterminatezza del programma sia effettivamente fondato o meno.

Nel tentativo di trovare delle risposte, bisogna guardare a quello che viene definito come il <<punto di congiunzione tra le due fattispecie>>[162]: il concorso di persone nel reato continuato, ossia l'ipotesi in cui i concorrenti decidano di commettere una serie di reati in momenti successivi, con caratteristiche tali da far pensare che siano legati da un medesimo disegno criminoso[163], focalizzandosi sui ragionamenti eseguiti da dottrina e dalla giurisprudenza sul punto.

Un autorevole pensiero[164] riporta che la distinzione tra le fattispecie di concorso di persone nel reato continuato e nell'associazione a delinquere si fonda solo sulla tipologia di programma: nel caso dell'associazione a delinquere il programma è di tipo <<generico>>, invece nel concorso di reati continuati il programma è <<circoscritto alla realizzazione di reati <<determinati>>>>[165]. Al fine di distinguere le due fattispecie, si dovrebbe pertanto ricercare la presenza o meno di questa indeterminatezza.

Tuttavia, per vedere se davvero la distinzione si basa solo sull'elemento del programma, si presenta una situazione molto più complessa di quello che sembra.
Partendo dall'analisi degli elementi caratterizzanti il fatto tipico dell'art.416 c.p., si deve far notare come la giurisprudenza per lungo tempo (ai fini dell'individuazione di quest'ultimo) abbia fatto affidamento sui requisiti del vincolo associativo e sul programma delittuoso: se per il secondo è da sempre stata punto di riferimento la caratteristica

[161]Insolera, *op. cit.,* pag. 114.
[162]*Ibidem.*
[163]Misaggi, *op. cit.,* pag. 91. Il <<disegno criminoso>> consisterebbe, a detta dell'Autrice, in <<un'iniziale programmazione e deliberazione generica di compiere una pluralità di reati, già originariamente preordinati alla realizzazione di un unico fine prefissato e sufficientemente specifico.>> Di conseguenza il soggetto, proprio perché mosso dall'intento di realizzare il disegno criminoso, commetterebbe solo una volta un motivo a delinquere. Questo farebbe emergere la caratteristica della <<unicità dello scopo>> per la fattispecie di reato continuato, creando di conseguenza un avvicinamento tra la posizione psicologica di colui che agisce ex art 81^2 c.p. ed il dolo specifico del partecipe ad un'associazione per delinquere.
[164]Del Corso, *I nebulosi confini tra associazione per delinquere e concorso di persone nel reato continuato*, (nota alla sentenze: Cass. pen. Sez. I, 30/04/1979, Reale, in *Giust. Pen.,* 1979, vol. II; Cass. pen., Sez. I, 28/03/1979, Pizzo, in *Riv. Pen.*, 1980, pag. 83), in *Cass.Pen.,* fascicolo 4/1985, pag. 623.
[165]Cass. Pen., Sez. I del 28/03/1979, Pizzo, in *Riv. Pen.,*1980, pag. 83.

dell'indeterminatezza, per il primo invece si è di fatto oscillato tra la caratteristica della <<permanenza>> ed <<il carattere generale e continuativo>>[166].

Focalizzandosi su questi due elementi del fatto tipico, alla dottrina[167] risulta esser piuttosto evidente che la permanenza del vincolo non può non derivare dalla stessa indeterminatezza del programma: per distinguere le due fattispecie, non ci si può basare su una mera divisione dei compiti, perché è un aspetto comune ad entrambe le fattispecie; piuttosto, bisogna riagganciarsi al carattere dell'indeterminatezza del programma associativo per trovare la permanenza nel tempo del vincolo associativo. Solo in questo modo l'associazione diventa <<accordo rivolto alla realizzazione di una serie indeterminata di reati>>[168].

Ora, per inquadrare meglio la distinzione del programma rispetto al disegno criminoso, si deve menzionare un ragionamento posto dalla giurisprudenza: affinché si realizzi l'elemento della continuità tra più reati, è necessario <<la rappresentazione fin dall'inizio, dei singoli episodi criminosi, individuati almeno nelle loro linee essenziali>>[169].

Tenuto conto di quest'elemento, viene subito in mente una domanda più che legittima: come bisognerebbe qualificare allora un programma delittuoso dove, sin dall'inizio, viene programmato ogni dettaglio?
Può essere data una spiegazione con la riforma dell'art. 81 c. p., introdotta dalla L.7 giugno 1974, n. 220, che pone nella fattispecie il requisito dell'omogeneità delle violazioni: questo ha fatto sì che per l'individuazione del concorso di persone nel reato continuato divenuta caratteristica essenziale l'unità del disegno criminoso, ossia la rappresentazione indicata sopra .

Questo ha creato non poca confusione: da un lato, questa riforma ha aperto <<una prospettiva di maggiore genericità programmatica>>[170] per il reato continuato; dall'altro lato si è dato vita ad un vero e proprio correre ai ripari della giurisprudenza, col tentativo di

[166]Del Corso, *op. cit.,* pag. 623. Inoltre, l'Autore segnala anche la presenza di un ramo della giurisprudenza che individua ulteriormente la necessità del requisito dell'organizzazione: sulla controversa natura della struttura organizzativa dell'associazione, si veda il paragrafo 2 c). Per una visione più generale, si veda: Fiandaca, Musco, *op. cit*., pag. 511.
[167]*Ibidem.*
[168]*Ibidem.*
[169]Cass. Pen., Sez. V del 25/11/2000, in *Giur. It.,* 2003, fasc. 8/9, pag. 510.
[170]Del Corso, *op. cit*., pag 344.

utilizzare il requisito dell'organizzazione[171] come elemento scernente l'associazione a delinquere e il concorso di persone . In questo modo si è perso l'immediato collegamento del requisito della stabilità del vincolo associativo con l'indeterminatezza del programma, sostituendo il secondo elemento di questa relazione con la struttura organizzativa.

In definitiva, tramite il sacrificio dell'elemento d'indeterminatezza del programma a favore del requisito dell'organizzazione, <<il reato associativo divenga funzione dei delitti programmati>>[172]: quest'oscuramento dell'indeterminatezza del programma non solo avrebbe creato maggior nebulosità sugli elementi costituenti il fatto tipico, ma anche avrebbe tolto al programma <<quel *minimum* di maggiore concretezza insito nella predeterminazione dei fatti oggetto del programma>>[173].

In conclusione a questa disamina dell'elemento dell'indeterminatezza del programma, emerge anche come la vaghezza dell'elemento del programma criminoso determini una vera e propria dipendenza dall'elemento organizzativo del fatto tipico , come lo è stato anche per il vincolo associativo. Si rende o dunque ancor più evidente l'urgenza di un recupero approfondito e soprattutto chiaro dei requisiti fondamentali del fatto tipico della fattispecie associativa, sia dal Legislatore ma - si aggiunge- anche dalla dottrina e dalla giurisprudenza.

2.3. La struttura organizzativa

Bisogna, infine, trattare l'ultimo elemento caratterizzante il fatto tipico de l'associazione a delinquere semplice, forse definendolo anche come quello più controverso. Infatti, la difficoltà più evidente riguardo l'organizzazione si trova già nella difficoltà d'inquadramento di questa di questo concetto nella fattispecie.

Un primo tracciamento della nozione di organizzazione dotata di stabilità può essere il definire essa come <<il collegamento logico, […] di tipo "dinamico", fra questi "insiemi"

[171]Per i diversi significati attribuiti alla nozione di organizzazione, si veda il sottoparagrafo 2.3. .
[172]Del Corso, *op. cit.,* pag. 343.
[173]De Francesco, *op. cit.,* pag. 61. V. anche : Cass. pen., Sez. I, n.66/1997, Ciampà, in *Cass. Pen.,* 1998.

[ossia, una pluralità di persone e l'attività delittuosa (costituita da più delitti), N.d.A.] >>[174].

Inoltre, si può introdurre che l' elemento organizzazione è composto da due elementi: da un lato dalle convenzioni di carattere generale, dall'altro <<dalla reciprocità degli impegni e quindi delle aspettative circa la distribuzione ed il coordinamento delle funzioni […], in ordine al concreto svolgimento di un'attività>>[175].

Quest'ultima precisazione fa sorgere un aspetto che dev'esser colto**:** è così importante l'aspetto della distribuzione dei compiti e delle funzioni affinché sussista l'organizzazione? O, formulando la domanda più in generale: quali sono i requisiti che, in concreto, permettono di verificare la sussistenza dell'elemento dell'organizzazione ex art. 416 c.p.? Per tentare di affrontare questa spinosa tematica, bisogna analizzare con attenzione gli orientamenti della giurisprudenza che si sono susseguiti nel tempo e i diversi pensieri della dottrina al riguardo.

1. Un primo orientamento ha posto l'accento sulla necessità di una struttura che sia <<idonea ed adeguata alla complessità del programma criminoso>>[176]. Ai fini della sussistenza dell'organizzazione, sarebbe dunque più che sufficiente la presenza di un <<minimum d'organizzazione a carattere stabile>>[177], essendo indifferente la sussistenza di una struttura complessa, con le conseguenti ripartizioni di funzioni e competenze tra gli associati . Infatti, secondo quest'orientamento basta <<una semplice e rudimentale predisposizione di mezzi»[178], ossia strumenti già esistenti che siano bastevoli per perseguire concretamente quel programma criminoso.

Tuttavia, la dottrina ha posto non poche critiche a questa posizione, di cui se ne segnalano nello specifico due.

[174]Aleo,*op. cit.,*pag.174.
[175]*Ibidem.*
[176]Burzi, *op. cit.* , pag. 1485.
[177]La definizione si riprende da: Borsari, Provolo, *op. cit*., pag.38. Nello stesso senso: Consulich, *op. cit.,* pag.114. Per la giurisprudenza: Cass. pen. Sez. I del 13/01/1983, in *Giur. It*.,1983, Vol.II, pag.353; Cass. pen. sez. II del 08/07/1983,in *Cass.Pen*., 1985, pag. 866; Cass. pen. sez. VI n. 3886/2011, in C.E.D. Cass. 2011; Cass. pen. sez. II, n. 20451/2013, in C.E.D. Cass. 2013.
[178]Cass. pen. Sez. I, cit., 5/12/1994, Semeraro. Si veda pure: Cass. pen. sez. I del 26/10/1977, in *Cass.Pen*., 1979, pag.306; Cass. pen. sez. I del 16/11/1984, in *Giust. pen*., 1985, Vol. II, pag.616; Cass. pen. sez. I del 05/12/1994, in *Cass. Pen*. 1996, pag.77.Cass. pen. sez. I del 27/02/1993, in *Giur. It.* 1994, Vol. II,pag. 672.

Con la prima, si va a sottolineare come con questa posizione si rischia di <<ricondurre all'art-416 c.p. associazioni strutturalmente inidonee a mettere in pericolo l'ordine pubblico>>[179].

Nella seconda, viene definito l'accostamento dei termini organizzazione e rudimentale addirittura come <<una sorta di ossimoro>> [180] : se infatti lo stesso concetto d'organizzazione richiama il concetto di una struttura complessa ed articolata, invece l'aspetto del rudimentale conferisce alla struttura la mera consistenza di un semplice gruppo che, d'intesa, si muove insieme. Di conseguenza, affermare che sia sufficiente un'organizzazione solo di carattere rudimentale, <<significa, di fatto, negare che quello dell'organizzazione sia davvero un requisito dell'associazione>>[181].

Sviluppando il ragionamento sulla base di quest'ultima critica, parrebbe evidente che questo requisito della rudimentale predisposizione di mezzi non è bastevole persino per la stessa giurisprudenza, poiché vi sono numerose pronunce poste nel tempo che, anziché esplicare cosa si intenda davvero per <<rudimentale predisposizione di mezzi>>, manifestano invece la tendenza ad esprimere <<ciò che "non serve" perché si possa parlare di organizzazione>>[182].

Tutte queste sentenze volte ad identificare gli aspetti negativi dell'elemento organizzativo hanno probabilmente contribuito alla graduale formazione di un ulteriore orientamento interpretativo. In particolare, si è negata la necessità del requisito dell'organizzazione, sostenendo invece l'adeguatezza dell'*affectio societatis scelerum* (il <<vincolo associativo esteso ad un programma indefinito di reati>> [183]). Di conseguenza, seguendo il ragionamento posto da queste pronunce, sarebbe irrilevante considerare la presenza di gerarchie interne e la suddivisione di ruoli[184].

---

[179]Fiandaca, Musco, *op. cit.,*pag. 511.

[180]Corvi, *Alla ricerca del "fatto" penalmente rilevante nei delitti associativi* (nota alla sentenza Cassazione penale, sez. V n.695 del 03/12/2013),in *Riv. It. Dir. e Proc. Pen.*, 2015, fasc. 1, pag. 380.

[181]*Ibidem.*

[182] Si fa riferimento alle pronunce: Cass. pen. sez. VI n. 5500/1998, in C.E.D. Cass. 1998, in cui si evidenzia come non serva tanto la presenza di gerarchie o di una distribuzione di ruoli, essendo piuttosto bastante<< l'esistenza di un vincolo non circoscritto a determinati delitti ma esteso ad un generico programma delittuoso>>; Cass. pen. sez. I n. 17027/2003, in *Cass. Pen*. 2004, pag. 2346, dove emerge la non indispensabilità di una struttura gerarchica affinché si prospetti il requisito dell'organizzazione. (spostato in nota)

[183]Cass. pen. sez. II del 15/04/1986, in *Riv. Pen*., 1986, pag.955. Nello stesso senso: Cass. pen., Sez. I del 01/07/1988, in *Giust. Pen*., 1989, Vol. II, pag. 535; Cass. pen. sez. I del 25/05/1990, in *Cass. pen.* 1992, pag.300; Cass. pen. sez. VI n. 5500 /1998, in C.E.D. Cass. 1998.

[184]Si veda: Tona, *op. cit.,*pag.1083.

2. Si è poi affermato un canale giurisprudenziale in cui ci si focalizza sulle indispensabili caratteristiche della stabilità ed operatività dell'organizzazione, «allo scopo di realizzare un programma criminoso protratto nel tempo, con ripartizione di compiti tra gli associati»[185]. Conseguentemente, per questa corrente non sarebbe necessaria un'esplicita manifestazione di volontà per la formazione del vincolo associativo[186].

3. Infine, le pronunce richiamate poc'anzi nell'escludere ciò che non configuri un'organizzazione rudimentale hanno probabilmente contribuito alla graduale formazione di un ulteriore orientamento interpretativo.
   In particolare, si è negata la necessità del requisito dell'organizzazione, sostenendo la sufficienza dell'*affectio societatis scelerum* (il <<vincolo associativo esteso ad un programma indefinito di reati>> [187]). Di conseguenza, era irrilevante considerare la presenza di gerarchie interne e la suddivisione di ruoli[188].

L 'origine di queste tendenze giurisprudenziali son probabilmente da ricercare nella confusa attività di valutazione del dato organizzativo da parte della giurisprudenza [189]. Nello specifico, è avvenuta una vera e propria sostituzione del <<l'oggetto di verifica dell'accordo**>>**[190]: oltre a svincolare l'organizzazione dalla gerarchia, dalla suddivisione in ruoli, dalla presenza di precise regole o dall'esser dettagliatamente predeterminata, è avvenuto un vero e proprio **s**vilimento del dato organizzativo, collocandolo nel vincolo associativo esteso ad un generico programma delittuoso: questo farebbe aumentare il rischio sia di eliminare la distinzione tra l'associazione per delinquere e il concorso di persone nei reati-fine, che di arrivare alla constatazione che <<l'accordo è nozione indubbiamente oggettiva>>[191].

Davanti a questi diversi orientamenti giurisprudenziali, la dottrina ha posto diverse argomentazioni, allo scopo di trovare una adeguata definizione dell'organizzazione che allo stesso tempo mantenga il requisito d'offensività della fattispecie. A questo scopo, si è

---

[185] Cass. pen. sez. V n. 10076/1998, in *Cass. Pen*.2000, pag. 1946. dove la focalizzazione sulle caratteristiche della stabilità ed operatività dell'organizzazione sono eseguite solo con la mera finalità di «realizzare un programma criminoso protratto nel tempo, con ripartizione di compiti tra gli associati».
[186] Burzi, *op. cit.,* pag.1485.
[187]Cass. pen. sez. II del 15/04/1986, in *Riv. Pen*., 1986, pag.955.
Nello stesso senso: Cass. pen., Sez. I del 01/07/1988, in *Giust. Pen*., 1989, Vol. II, pag. 535; Cass. pen. sez. I del 25/05/1990, in *Cass. pen*. 1992, pag.300; Cass. pen. sez. VI n. 5500 /1998, in C.E.D. Cass. 1998.
[188]Si veda:Tona, *op. cit.,*pag.1083.
[189]*Ibidem*. Per maggiori approfondimenti sul punto,si fa riferimento a: Del Corso, *op. cit.,* pagg.624-625.
[190]*Ibidem.*
[191]*Ivi,*pag. 1084.

elaborato il concetto di idoneità dell'organizzazione. Come appunto definito da un pensiero pressoché unanime[192], se infatti non si considerasse questa stessa, si desumerebbe la pericolosità per l'ordine pubblico dalla sola esistenza dell'accordo criminoso: cosa che, per le critiche viste in precedenza, non è in alcun modo accettabile.

Ma in cosa deve consistere quest'idoneità? Vi sono due posizioni generali della dottrina sulla questione:

- Un primo ramo della dottrina, considera l'idoneità dell'organizzazione deve consistere nel requisito che l'associazione abbia una struttura tale da poter già consentire la piena attuazione dello <<scopo di commettere più delitti>>, e di poter dunque potenzialmente mettere in pericolo i beni giuridici minacciati dagli stessi reati-scopo[193];
- Un altro ramo della dottrina [194] (quello maggioritario) vede piuttosto nell'idoneità dell'organizzazione l'adeguatezza della stessa alla realizzazione del programma delittuoso: così come l'associazione a delinquere si estingue quando il programma diventa per essa irraggiungibile, così deve considerarsi esistente quando ha una struttura complessa, che le permetta la potenziale attuazione del programma stesso[195].

Viene però fatto notare, secondo un autorevole ragionamento di un ramo della dottrina[196], come accogliere una tesi piuttosto che l'altra è perlopiù indifferente, perché il risultato sarà sempre lo stesso. Questo viene dimostrato dal fatto che si possono verificare due alternative:

a) Si prende come riferimento i beni tutelati rispetto ai reati-scopo: l'idoneità a ledere gli stessi corrisponde al concetto d'idoneità a concretizzare il programma criminoso - che ha appunto come oggetto i delitti-scopo;
b) Si prende come riferimento un bene giuridico tutelato, diverso da quelli dei reati-scopo. Questo altro non può essere se non lo stesso ordine pubblico, il bene giuridico protetto dallo stesso art. 416 c.p.:l'associazione potrà essere considerata pericolosa per

[192]Si veda: Borsari, Provolo, *op. cit*., pagg.39-40; Fiandaca, Musco, *op. cit.,* pag. 511; Insolera, *op. cit*., pag. 91 e ss.
[193]Insolera*, op. cit*., pag. 92.
[194]Si cita, ad es.: Borsari, Provolo, *op. cit*., pag.38-39; Fiandaca, Musco, *op. cit*., pag. 511; Patalano, cit.,*op. cit*., pag. 92.
[195]*Contra:* Insolera,*op. cit*., pag.92, il quale ritiene che, nonostante questa tesi abbia <<il pregio di cercare una definizione dell'elemento oggettivo del reato con strumenti ermeneutici rigorosamente applicati alla fattispecie>>, non riesce a cogliere il vero obiettivo: il conferire autonomia al concetto di associazione, e per fare ciò non si può certo riferirsi alla consumazione dei delitti-scopo.
[196]Corvi, *op. cit.,* pagg. 384 e ss.

l'ordinamento solo <<presentandosi idonea ad agire secondo i suoi orientamenti, ossia secondo il suo piano>>[197].

In chiusura sul rapporto tra il concetto di idoneità ed organizzazione, si può desumere che:

- A prescindere dal significato che si accolga per il concetto di idoneità, è importante che essa non vada intesa solo in senso statico (ossia, solo in riferimento ai mezzi a disposizione dell'associazione), ma vada intesa in senso dinamico, comprendendo dunque anche la capacità di impiego degli stessi, <<dal momento che l'organizzazione non ha solo componenti materiali, ma pure intellettuali>>[198].
- L'idoneità deve contribuire alla creazione di una nozione <<'forte' di organizzazione>>[199]: l'organizzazione deve quindi necessariamente ripartirsi i compiti (conseguentemente, anche poi i ruoli e competenze) tra gli associati, nonché dev'esser dotata un'opportuna messa a punto dei mezzi. Tutti questi elementi sono necessari per <<la costituzione, il consolidamento, e poi, al mantenimento in vita ed al rafforzamento dell'ente in quanto tale>>[200] .

Da questa parentesi emerge una caratteristica molto importante dell'organizzazione, ossia la sua elasticità: per quanto l'organizzazione debba esser complessa, non si deve immediatamente pensare che vi siano parametri rigidi per ritenere sussistente l'elemento organizzativo, e che essi siano validi per qualsiasi tipologia d'associazione a delinquere.

Considerata la *ratio* del Legislatore di considerare l'atto dell'associarsi come <<una forma libera, decisa di volta in volta dagli individui, singolarmente e collettivamente, a seconda delle […] esigenze operative e programmi perseguiti>>[201], la giurisprudenza ha assunto la tendenza non di utilizzare un modello prestabilito di organizzazione, ma quella di far assumere alla nozione caratteristiche diverse a seconda della causa in decisione[202].

---

[197]Leo, *L'associazione a delinquere finalizzata al traffico di stupefacenti (Art. 74 D.P.R. n. 309/90)*, in Cadoppi, Canestrari, Manna, Papa, *Trattato di Diritto Penale*, *Parte Speciale*, Vol. IV, UTET Giuridica, 2010, pag.702 e ss.

[198]Cavaliere, *Tipicità ed offesa nei reati associativi*, in Patalano (a cura di), *Nuove strategie per la lotta al crimine organizzato transazionale*, Giappichelli, 2003,pag.89.

[199] Corvi*, op. cit.,* pag. 385

[200]De Vero, cit., *I reati associativi nell'odierno sistema penale,* in *Riv. It. Dir. e Proc. Pen.,* 1998, pag. 389 e ss. Nello stesso senso: De Francesco, *Societas Sceleris*, pag. 108; Id., *(voce)Associazione per delinquere*, pag.297; Tona, *op. cit*., pag. 1083; Muscatiello, *Il concorso esterno nelle fattispecie associative,* CEDAM, 1995, pag.36..*Contra*: Iacoviello, *op. cit.,* pag.58.(spostato dalla nota di sopra a quella di sotto)

[201]Tona, *op. cit*., pag. 1083

[202]Si fa riferimento a:Cass. pen., cit., Sez. I n. 34043/2006, in *Riv. Pen*. 2006, pag. 663. Nello stesso senso: Corvi,*op. cit.,* pag.384 . V. anche Muscatiello, *op. cit*., pag. 40, che evidenzia il fatto che oggi si tende a

Si realizza in questo modo un processo di <<gradualità specializzante>> della nozione associativa, tale da renderla più duttile all'interno dell' art. 416 c.p. ma allo stesso tempo più distante rispetto alle nuove esigenze di tutela sociale.

Questo non solo crea problemi sul piano probatorio per la distinzione tra concorso e associazione, ma crea, più in generale, delle problematiche sul piano organizzativo a livello probatorio: non sono stati pochi i casi in cui la giurisprudenza[203] ha ribaltato il rapporto tra organizzazione e delitti-scopo, utilizzando il numero dei delitti-scopo come elemento per desumere la presenza dell'organizzazione, non il contrario. Per cui, la vaghezza del termine incide inevitabilmente sul piano probatorio per la stessa individuazione dell'organizzazione.

Sulla base di quanto detto finora, seppur sia indubbio che: non possa esistere una nozione unitaria e costante di organizzazione, odiernamente vi è un'emersione sempre più variegata di diverse tipologie di organizzazioni, nonché che la struttura dell'organizzazione muti a seconda del tipo di programma da attuare[204]; si deve necessariamente concludere che l'idoneità a realizzare il programma (o, se si preferisce, a ledere il bene o i beni giuridici) <<finisce per essere l'inizio e la fine del requisito dell'organizzazione, rischiando di svuotarlo di fatto di contenuti afferrabili>>[205] . Focalizzarsi solo sul numero e tipologia di delitti che si vuole porre in essere rende di fatto l'apparato organizzativo in "forme" di carattere infinito e dai contorni sfumati.

Può sorgere spontaneo chiedersi se vi siano allora altri requisiti caratterizzanti l'organizzazione oltre l'idoneità, al fine di dare maggiore consistenza all'elemento organizzativo e poter agevolare la sua individuazione nella vita quotidiana.
Alcuni studiosi[206], per individuare meglio il concetto di organizzazione, sulla base di un'attività comparativa tra la dottrina e della giurisprudenza tedesche (più precisamente, ai paragrafi 129 e 129a StGB)[207] e le fattispecie associative presenti nel Codice Penale

---

considerare la nozione dell'associazione non tanto sulla base del dato normativo, quanto piuttosto <<sulla maggiore o minore opportunità di tutela avverso quei comportamenti ritenuti socialmente sanzionabili>>.
[203]App. Catanzaro, sez. I, del 2/2/1985 in *Cass.Pen.*, 1985.
[204] In questo, si fa rinvio al sottoparagrafo 2.3. di questo capitolo, guardando al legame tra specificità del programma delittuoso ed idoneità dell'organizzazione criminosa individuato da Iacoviello,*, op. cit.,* pag.58.
[205]Corvi, *op. cit.,* pag.384.
[206]*Ivi,*pag.387.
[207] In essi si enuncia che, affinché possa sussistere un'associazione a delinquere, debbono esser cumulativamente presenti questi requisiti:

italiano, hanno ritenuto che, oltre l'idoneità, gli elementi essenziali del fattore dell'organizzazione potrebbero essere:

a) Una normativa interna. L'organizzazione dovrebbe avere delle proprie regole, riguardanti: l'ingresso nell'associazione; la modalità di formazione della volontà dell'associazione (le decisioni vengono prese dai vertici dell'associazione, ovvero da tutti gli associati, tramite voto all'unanimità o a maggioranza); regole di condotta nei rapporti fra loro o con terzi; nonché il c.d. <<vincolo all'obbedienza>>[208]: ciascun partecipante dovrebbe obbligarsi a prestare il proprio contributo alle decisioni prese nel rispetto della modalità di formazione della volontà comune scelta, anche nel caso in cui il partecipante abbia manifestato dissenso a quella stessa decisione.

b) Una strutturazione interna su più livelli. Quest'elemento, a differenza del precedente, viene tratto, dalle fattispecie associative incriminate nel codice penale italiano: dato che in esse risultano previste, accanto alla figura del partecipe, le c.d. partecipazioni qualificate (ad es.: l'organizzatore, il capo, il promotore, ecc.) è un chiaro segnale posto dal legislatore sull'importanza di una struttura di tipo gerarchico per l'associazione a delinquere, <<con capi che danno ordini e semplici partecipi che li eseguono, ed una serie di 'ruoli istituzionali', funzionali alle esigenze 'vitali' dell'ente stesso>>[209].

c) L'articolazione in una serie di ruoli, distinguibili, a livello approssimativo, in due categorie: i ruoli apicali(<<ricoperti da chi pone in essere le attività più importanti per l'esistenza ed il funzionamento dell'ente>>, in grado di impartire ordini agli altri partecipanti), ed i ruoli subalterni, propri di chi si obbliga <<ad agire quotidianamente per garantire la sopravvivenza dell'organizzazione>>[210].

Da questa disamina emerge come il mero focalizzarsi sul criterio dell'idoneità non è sufficiente a garantire un recupero completo del concetto di organizzazione: solo con la

---

- un sodalizio di almeno tre persone,in grado di durare nel tempo per il perseguimento di uno scopo comune,
- la presenza di precise regole di appartenenza, che permettano d'identificare chiaramente tutti gli associati. Queste regole devono inoltre esser vincolanti, poiché devono essere il mezzo di formazione d'una volontà comune,
- la sottomissione dei partecipi a quella stessa volontà comune.

[208]Corvi, *op. cit.,* pag.386.

[209]*Ivi,*pag.. 387. *Contra:*Manzini,*Trattato di diritto penale italiano,*(agg. a cura di) Nuvolone e Pisapia, UTET , 1981.

[210]*Ibidem.*

presenza simultanea di questi altri elementi si permette la realizzazione di <<nozione 'forte' di associazione>>[211] nella fattispecie, garantendo. anche il recupero dell'autonoma incriminazione dell'articolo 416 c.p. .

Ora, in chiusura di questo paragrafo, si deve necessariamente esser d'accordo su quanto detto dalla dottrina sulle conseguenze della varietà delle tipologie di associazioni a delinquere ricadenti sul requisito dell'organizzazione: nonostante l'oggetto della trattazione sia solo rivolto alle associazioni a delinquere semplici, è indubbio che il costante, veloce sviluppo e diffusione di sempre più diverse tipologie delle associazioni a delinquere comporta che non sia possibile trovare una definizione univoca di associazione.

Tuttavia, nonostante si apprezzi il tentativo di trovare ulteriori elementi rispetto l'idoneità caratterizzanti l'organizzazione, sono sorti alcuni dubbi, che possono esser tenuti in considerazione:

- Qualora l'ente in questione (oltre l'idoneità) non abbia tutti gli elementi indicati sopra si dovrebbe comunque considerare sempre la presenza dell'organizzazione (e quindi, prevedere l'applicazione dell'art. 416), oppure questa si dovrebbe escludere? Ad esempio: rientrerebbe nell'art.416 un gruppo di presone che non hanno una struttura interna ben precisa, ma hanno a disposizione mezzi e persone sufficienti per l'attuazione del loro programma? O ancora, nel caso in cui vi fosse sì una struttura, ma non vi fosse una specifica normativa regolante l'entrata di nuovi membri o delle regole di condotta?
  Forse considerare come <<nozione 'forte' dell'associazione>>la presenza simultanea di tutti gli elementi individuati non solo sembrerebbe far venire meno quella flessibilità del concetto di organizzazione (che, come visto, non è elemento da sottovalutare); ma anche rischierebbe di non far rientrare nell'art. 416 numerose situazioni, lasciandole del tutto impunite.

- La dottrina ha inoltre posto una grande attenzione verso il <<vincolo dell'obbedienza>>, consistente nell'obbligo dei partecipanti all'esecuzione della volontà comune dell'associazione, anche qualora gli stessi non fossero d'accordo con la singola decisione.

[211] *Ibidem.*

Questo, però, andrebbe contro lo stesso concetto di autonomia della fattispecie associativa, in base al quale il soggetto è considerato responsabile penalmente ex art. 416 c.p. per la sola partecipazione all'associazione, anche qualora non abbia contribuito in alcun modo alla realizzazione del programma.

Ad ogni modo, sulla base di quanto visto finora, il contenuto della nozione d'organizzazione rimane ancora una questione su cui sia dottrina e giurisprudenza devono ancora continuare a confrontarsi, a maggior ragione (come si ben vedrà) considerando gli innumerevoli modi in cui l'organizzazione e l'associazione stessa prendono vita nella realtà.

3. Le condotte associative

3.1. La controversa definizione della condotta di partecipazione

Un primo dato da fornire per l'inquadramento della condotta di partecipazione è la caratteristica di esser a forma libera[212]: per la dottrina è pertanto possibile consentire l'applicazione dell'art. 416 c.p. a <<qualsiasi ipotesi di contributo, […] alla realizzazione dell'evento o al protrarsi della situazione antigiuridica da quest'ultimo ingenerata>> . In questo modo, la costruzione ampia della condotta di partecipazione fa sì che essa possa manifestarsi con diverse modalità, purché sempre causalmente rilevanti.

In particolare, viene inquadrata la figura del partecipe come una categoria residuale rispetto alle altre condotte qualificate: non può infatti esser ricondotto ad esso il ruolo di un <<mero <<strumento>> destinato all'attuazione degli scopi associativi>>[213], perché si rischierebbe di comparare il partecipe a qualsiasi mezzo di cui l'associazione dispone. Bisognerebbe, piuttosto, riconoscere a quest'ultimo<<un ruolo necessariamente "attivo">>[214] , ossia la sua capacità di contribuire alla vita dell'associazione perché in grado di <<orientare l'attività associativa verso la realizzazione degli scopi>>[215], al pari delle condotte qualificate.

Ora, nonostante queste importanti definizioni sovra citate, è chiaro che i contorni del concetto di partecipazione rimangono ancora sfumati: la giurisprudenza si è sforzata di trovare una strada che permettesse di fornire maggior concretezza al concetto, ma senza allo stesso tempo negare le caratteristiche della forma libera e della residualità viste sopra.

Sulla base degli studi svolti[216], si è potuto suddividere gli indirizzi della giurisprudenza in tre macrocategorie, relative ai diversi criteri utilizzati per l'individuazione della condotta di partecipazione:

1. Il c.d. criterio causale: caratteristica di questa categoria è quella d'incentrare l'identificazione della partecipazione sulla c.d. <<attualità del contributo>>[217], ossia è

[212]Insolera, *op. cit.,* pag. 204. Nello stesso senso: Cass. pen. Sez. II, n.49691/2004 in *Dir. Pen. e Proc*., n. 5/2005, pag. 593;Cass. pen. sez. I del 27/01/1986, in *Cass. pen*., 1987, pag. 1719.
[213] De Francesco, *Societas Sceleris.Tecniche repressive delle associazioni criminali,* in *Riv. it. di Dir. e Proc. Pen.,* 1992, vol. I, pag. 141.
[214]*Ivi,* pag. 142.
[215]*Ibidem.*
[216]Per la stesura di questo sottoparagrafo è stato molto utile riprendere il lavoro di: Fiandaca e Musco,*op. cit.,* pagg.508 e 509, Borsari, Provolo, *op. cit.,* pagg. 44 e 45.

sufficiente la presenza di un contributo casualmente rilevante per il funzionamento dell'associazione,<<a prescindere dal ruolo o dal compito che il partecipe svolge nell'associazione>>[218].

Questa corrente di pensiero è sostenuta ampiamente sia da un ramo della dottrina che della giurisprudenza[219]. Accennando alla prima[220], si ammette la possibilità di una nozione di c.d. <<causalità della partecipazione>>[221], alla presenza però di due condizioni:

- Essa deve essere intesa non come una *condicio sine qua non* . Piuttosto, la condotta di partecipazione deve esser rivolta a consentire che venga incrementata <<in modo empiricamente verificabile, rispetto alla situazione anteriore, la pericolosità della concreta organizzazione.>>[222].
- È necessario anche l'aspetto della stabilità, ossia l'estensione della condotta partecipativa nel tempo,in grado di creare un <<disvalore d'azione che corrisponda a quello di evento>>[223].

Riguardo a questa posizione vi sono state però anche delle critiche. Guardando sommariamente due tra queste:

- *in primis* si precisa come l'accoglimento di questa posizione comporterebbe la degradazione della condotta in un'entità <<puramente materiale>>[224];

- Nonostante venga riconosciuto che tramite questo approccio sia possibile misurare la pericolosità del comportamento del soggetto[225], l'applicazione di questo criterio crea non

---

[217]La definizione si trae da: Muscatiello, *op. cit.,* pag. 44.

[218]Borsari e Provolo, *op. cit*., pag.44. Gli Autori precisano però, nella stessa pag., che, invece, sul piano probatorio, sia fondamentale specificare il tipo di ruolo o attività svolta dal partecipante nell'associazione, <<giacché altrimenti la previsione normativa non potrebbe sottrarsi a fondati rilievi di costituzionalità per l'assoluta carenza di tassatività del dato normativo>>. Nello stesso senso: Cass. pen. sez. I del 27/01/1986, in *Cass. pen*., 1987, pag. 1719. *Contra:* Cass. pen. sez. I del 21/02/1992, in *Giust. P*en., 1992, Vol. II, pag. 428. Inoltre, Fiandaca e Musco, *op. cit.,* a pag. 508, identificano che non necessariamente il contributo deve trattarsi strettamente di attività esecutive di tipo preparatorio dei delitti-scopo, riprendendo dunque il concetto di distinzione tra la responsabilità penale dei delitti-scopo e per la partecipazione dell'associazione a delinquere (si veda introduz. di questo paragrafo). Nello stesso senso: Tona, *op. cit.*, pag. 1099.

[219]Alcune sentenze a sostegno della posizione sono: Cass. pen. sez. III n. 47249/2014 in *Dir. & Giu*., 2014, 18/11; Cass. pen. sez. III n. 8024/2012, in C.E.D. Cassazione 2012; Cass. pen. sez. I del 13/06/1987 in *Cass. Pen*. 1988, pag. 1812.

[220]Cavaliere, *Il concorso eventuale nelle associazioni a delinquere e di tipo mafioso*, in : Picotti, Fornasari, Viganò, Melchionda, *I reati associativi : paradigmi concettuali e materiale probatorio. Un contributo all'analisi e critica del diritto vivente*, CEDAM, 2005, pagg. 130 e 131.

[221]Cavaliere, *op. cit*., pag.130.

[222]*Ibidem.*

[223]*Ivi,*pag.131.

[224]De Francesco, *op. cit.,* pag. 141.

[225]Tona, *ibidem*, a pagina 1101.

poche incertezze nella prassi, poiché è molto più difficile distinguere l'idoneità causale della condotta rispetto all'evento dal momento specifico in cui si forma il vincolo associativo[226].

2. Il criterio dell'inserimento organico: secondo quest'indirizzo, non è tanto importante la rilevanza causale della condotta, quanto piuttosto l'inserimento del soggetto all'interno dell'apparato organizzativo dell'associazione. Per parte della giurisprudenza, è necessaria l'ulteriore assunzione di << un profilo dinamico attinente alla partecipazione>>[227].La dottrina a supporto di questo criterio difende lo stretto legame tra l'inserimento organico nell'associazione e il concetto della condotta di partecipazione: a differenza del. precedente, esso è in grado di dare maggiore rilevanza penale alla condotta e rispetta meglio il principio di tipicità, dando maggior consistenza al significato di <<partecipazione>> nella fattispecie[228].

Tuttavia, non mancano le critiche in riferimento all'inserimento organico. Innanzitutto se, al fine di entrare a far parte dell'organizzazione, l'aspirante partecipe dovesse necessariamente manifestare un atteggiamento di adesione , seguito da un contestuale <<atto di accettazione>>[229] da parte degli altri associati[230]; sarebbe in realtà molto difficile dimostrare la presenza di <<un <<rituale>> di stabile e definitivo inserimento del compartecipe all'interno dell'organizzazione criminosa>>[231].

Inoltre, qualora venisse accolto questo criterio, è altamente probabile che la giurisprudenza individui lo stabile inserimento – e, conseguentemente, anche la condotta di partecipazione solo *<<per facta concludentia>>* [232] , ossia tramite altri esempi che

---

[226]Ingroia, *L'associazione di tipo mafioso,* 1993, Giuffrè, pag.41. Nello stesso senso: Muscatiello, *op. cit*., pag. 46.

[227]Cass. pen., Sez. Un., n.33748/2005 in *Foro It*., 2006, vol. II, pag. 86. Riprendendo il contenuto della sentenza: <<si definisce "partecipe" colui che, risultando inserito stabilmente e organicamente nella struttura organizzativa dell'associazione mafiosa, non solo "è" ma […]"prende parte" alla stessa: locuzione questa da intendersi non in senso statico, come mera acquisizione di uno status, bensì in senso dinamico e funzionalistico, con riferimento all'effettivo ruolo in cui si è immessi e ai compiti che si è vincolati a svolgere perché l'associazione raggiunga i suoi scopi, restando a disposizione per le attività organizzate della medesima.>>.V. anche : Cass pen. sez. I del 11/12/1992, in *Giust. Pen*., 1994, Vol. II, pag. 258.

[228]De Francesco, *op. cit.,* pag. 143. È corretto però specificare che, come si vedrà a breve, il suo risulta essere un accoglimento parziale della posizione.

[229]*Ivi,* pag. 142.

[230] V. pure Spagnolo, *L' associazione di tipo mafioso,* CEDAM,1993.

[231]De Francesco, *op. cit*., pag. 143. Nello stesso senso: Valsecchi, *Partecipazione e concorso eventuale nelle associazioni a delinquere diverse dall'associazione mafiosa*, in : Picotti, Fornasari, Viganò, Melchionda, *op. cit.,* pag.106.

[232]De Francesco, *op. cit*., pag. 143.

dimostrino la presenza di attività rivolte specificamente a sostegno dell'associazione a delinquere[233].

Da ultimo, è interessante vedere un'altra critica posta con riguardo ad un tema già trattato nell'ambito dell'aspetto dell'organizzazione vista precedentemente[234]: se, non può esistere ormai una nozione univoca di organizzazione per il mutamento della stessa struttura organizzativa in base <<alla natura dell'associazione criminosa di volta in volta considerata>> [235] e alla tipologia di programma criminoso mutando la tipologia di organizzazione, bisognerebbe forse elaborare anche una nozione diversa di partecipazione[236].

3. Una corrente giurisprudenziale più recente (e, al momento, predominante) accolta anche da parte della dottrina, ritiene doversi applicare il c.d. <<criterio <<misto>>[237]: affinché vi sia partecipazione ex art. 416 c.p. è necessario sia l'inserimento organico del soggetto,sia la sussistenza di un apprezzabile e concreto contributo causale all'esistenza o al rafforzamento dell'associazione criminosa.

Proprio riguardo quest'ultimo criterio, è utile osservare più da vicino una sentenza della Corte di Cassazione penale del 2004, ed il commento alla stessa[238]: seppur si tratta di reato di associazione a delinquere di tipo mafioso, in entrambi vi sono interessanti riflessioni di carattere generale sul concetto di partecipazione nell'associazione a delinquere semplice.

In sintesi, la controversia riguardava un importante esponente della politica italiana, accusato di partecipazione ad associazione a delinquere di tipo mafioso. Senza percorrere interamente tutto l'iter giudiziario, la Corte d'Appello di Palermo[239] aveva ritenuto provata la condotta partecipativa dell'imputato per il reato di associazione a delinquere ex art. 416 c.p. fino al 1980, assolvendo invece l'imputato per l'accusa di partecipazione ad

---

[233] Da quest'ultima riflessione, De Francesco, *op. cit.,* pag. 144 nota come questi due indirizzi finiscanosempre più per mischiarsi, in particolar modo sul piano probatorio: vi è dunque il rischio che nei processi venganoutilizzati i medesimi elementi di prova per provare la sussistenza della partecipazione sulla base di entrambi i criteri.

[234]Si fa, in particolar modo, riferimento al sottoparagrafo 2.3. di questo capitolo, pagg.42-43.

[235]Viganò, *Riflessioni Conclusive*, in *I reati associativi: paradigmi concettuali e materiale probatorio. Un contributo all'analisi e critica del diritto vivente*, (a cura di) Picotti, Fornasari, Viganò, Melchionda, CEDAM, 2005, pag. 309.

[236]*Ibidem.*.

[237] Sul punto v. Borsari e Provolo*, op. cit*., pag. 45.

[238]Corvi,*Requisiti e limiti della "partecipazione" nel reato di associazione a delinquere* (nota a Cass. pen. sez. II, n.49691/2004), entrambe in *Dir. Pen. e Proc*., 2005, n.5, pagg. 593-607.

[239]App. Palermo, n.1564/2003 in ArchivioAntiMafia.org

associazione mafiosa ex art. 416 bis c.p. per il periodo dal 1980 al 1992 . La sentenza di Cassazione riconfermò la sentenza d'appello, dimostrando la sussistenza della condotta partecipativa dell'imputato ex art. 416 bis, ma eseguendo non poche precisazioni, compreso il concetto di partecipazione all'associazione a delinquere ex art. 416 c.p.: se la sentenza d'appello si concentrava nel vedere la partecipazione solo nell'adesione psicologica, la Cassazione piuttosto identifica che è necessaria anche <<la concreta assunzione di un ruolo materiale al suo interno>>[240], richiedendo dunque la necessaria collocazione del partecipante all'interno dell'organizzazione in un ruolo specifico. In aggiunta, <<la manifestata disponibilità>> deve trovare <<concreta estrinsecazione attraverso comportamenti specifici>>[241].

Questa sentenza rientra quindi pienamente nel criterio <<misto>>, poiché tenta di ricondurre nella nozione sia l'inserimento organico nel vincolo associativo, sia l'elemento della rilevanza causale del contributo prestato dal soggetto per l'associazione a delinquere[242].

Pure questo criterio, però presenterebbe delle problematiche sul piano probatorio: osservato che la giurisprudenza << non ha mai […] formalmente abbandonato il riferimento alla natura causale di tale partecipazione>>[243], svuotandone il contenuto, si è sviluppato e si è largamente utilizzato nelle argomentazioni (come anche nella sentenza di cui sopra) il solo inserimento del partecipante nell'organizzazione come contributo rilevante per l'esistenza dell'ente. Da tutto ciò, si otterrebbe <<una presunzione *iuris et de iure*>>[244], secondo cui l'ingresso del sodalizio comporta automaticamente un contributo causale rispetto al rafforzamento dell'associazione .

La difficoltà, perciò, sta proprio sulle spalle del giurista: al fine di dimostrare a livello probatorio l'esistenza della condotta di partecipazione, egli dovrà dimostrare non solo l'inserimento stabile nell'organizzazione, ma anche ulteriormente la presenza di un contributo specifico e concreto, e soprattutto <<ulteriore rispetto alla mera inclusione dell'organigramma del sodalizio>>[245].

---

[240]Cass. pen. Sez. II, n.49691/2004 in *Dir. Pen. e Proc*., n. 5/2005, pag. 599.
[241]Cass. pen. Sez. II, n.49691/2004 in *Dir. Pen. e Proc*., n. 5/2005, pag. 597.
[242]Corvi, *op. cit.,* pag. 601.
[243]*Ivi*, pag.602.
[244]*Ibidem.*.
[245]*Ibidem*. Questo, nella stessa pag., comporta per l'Autrice l'utilizzo di materiale probatorio separato per dimostrare ciascun elemento: in caso contrario, <<il cumulo tra i due requisiti si rivelerebbe meramente fittizio, tornando così ad uno dei modelli di partenza: causale od organizzatorio […]>>.

Fatta quest'importante riflessione, sulla base di quali criteri nella sentenza in esame la Cassazione abbia visto un collegamento tra la condotta dell'imputato ed il concetto di partecipazione all'associazione a delinquere, analizzando da vicino sia il requisito organizzativo che quello causale:

1. Un primo dato da tenere in considerazione è che nella sentenza non vi sono elementi di prova sufficienti a disposizione della Cassazione che dimostrino un inserimento dell'imputato nell'apparato organizzativo dell'associazione[246].
   La Cassazione non dà appunto nel dispositivo alcuna spiegazione su quali siano gli elementi da cui si tragga la volontà dell'imputato di entrare a far parte del sodalizio criminoso o anche <<attivarsi in suo favore>>[247], tantomeno riguardo la volontà dell'associazione a far sì che l'imputato diventi un partecipe di essa.

2. Riprendendo la sentenza su cui si struttura il commento, l'evidenza casuale della condotta dovrebbe emergere da <<contributi <<effettivi, concreti e specifici>>>>[248], non essendo invece bastevole <<la mera vicinanza o disponibilità>>[249]. Gli elementi utilizzati dalla Cassazione nella sentenza a sostegno dell'accertamento della rilevanza causale della condotta dell'imputato sarebbero:

- I rapporti con l'imputato ed alcuni importanti esponenti di Cosa Nostra,
- I provati incontri dell'imputato nel biennio 1979-80 con il capomafia Bontate,
- La disponibilità dell'imputato all'ascolto delle richieste ed il generico impegno a soddisfarle (<< peraltro, in assenza di qualsiasi prova in ordine all'esecuzione della relativa "prestazione" o all'ottenimento di qualche beneficio da parte della mafia>>[250]),
- Il caso Mattarella: l'imputato non avrebbe denunciato i mandanti dell'omicidio, una volta avuta conoscenza delle loro intenzioni di commettere l'omicidio.

Partendo dal caso Mattarella, (riguardo il dato causale della condotta di partecipazione) non avrebbe alcuna rilevanza penale: né come reato omissivo proprio[251], poiché <<la

---

[246]Corvi, *op. cit.,*a pag. 603, fa anche riferimento al fatto che la sentenza App. Palermo, n.1564/2003 già aveva escluso che l'imputato fosse inserito organicamente nell'organizzazione mafiosa: <<deve pacificamente escludersi che le emergenze processuali consentano di ricondurre la figura dell'imputato a quella di "uomo d'onore", ritualmente ed organicamente affiliato a Cosa Nostra […] >>.

[247]Corvi, *op. cit.,*pag. 603.

[248]*Ibidem.*

[249]Cass. pen. Sez. II, n.49691/2004 in *Dir. Pen. e Proc.,* n. 5/2005, pag. 598.

[250]Corvi, *op. cit.,* pag. 604.

[251]Si ricorda che il reato omissivo si configura in tutti quei casi in cui il soggetto si astiene dal tenere un determinato comportamento previsto dalla legge. I reati omissivi si distinguono in propri ed impropri: per i primi, è sufficiente la sola condotta omissiva affinché vi sia responsabilità penale (esempio classico è il *reato d'omissione di soccorso,* ex art. 593 c.p.). Per i secondi, in base all'art. 40^2 c.p., è invece necessario che oltre la condotta omissiva, segua anche l'evento causalmente riconducibile alla condotta del soggetto (es. *omicidio*

mancata denuncia del cittadino - quale era l'imputato nel 1980 - integra gli estremi di un reato solo se ha ad oggetto, ex art. 364 c.p., un delitto contro la personalità dello Stato […]>>[252]; ma neanche come reato omissivo improprio: secondo la dottrina[253], il reato di favoreggiamento personale ex art. 378[1] c.p.[254] può esser commesso mediante omissione, ma è necessario che il soggetto si ritrovi in una c.d. posizione di garanzia, al pari di qualsiasi reato omissivo improprio.Considerato che questo stesso requisito sia essenziale anche per configurare <<una "partecipazione" al reato associativo tramite una condotta omissiva>>[255], si esclude che nel caso specifico vi sia la medesima posizione gravante sull'imputato[256].

Riguardo gli altri fatti, seppur da essi s'evincerebbe la presenza di un rapporto di vicinanza tra l'imputato e l'associazione a delinquere di tipo mafioso, non vi sono tuttavia elementi che dimostrino il concreto impatto della condotta dell'imputato come contributo alla vita dell'associazione stessa.

In via generale, non vi è nella sentenza:

- Alcuna traccia volta a provare che senza le condotte dell'imputato, l'associazione non avrebbe soddisfatto i propri scopi,
- Nessun <<giudizio controfattuale atto a dimostrare che, eliminate mentalmente queste condotte, l'associazione sarebbe stata materialmente diversa>>[257],
- Indicazioni di massime di esperienza, che, *de facta concludentia*, permettano di desumere che fatti simili comportino un effettivo beneficio all'associazione.

È interessante vedere come la Cassazione, nonostante abbia inizialmente posto l'enfasi sull'elemento organizzativo e causale per dimostrare la sussistenza della condotta di partecipazione, abbia alla fine fatto riferimento alla semplice disponibilità dell'imputato,

---

colposo derivante dall'omissione di un medico negligente): il soggetto in questo caso si trova in una c.d. posizione di garanzia. Quest'ultima, in generale, nasce o da una fonte normativa di diritto privato o pubblico (anche non scritta), o dall'esistenza di un potere (giuridico, ma anche di fatto). In base ad essa ai soggetti, in determinate situazioni, è affidata la protezione di determinati beni giuridici (un es. di posizione di garanzia è la *responsabilità genitoriale*). Per maggiori approfondimenti, si fa rinvio a: Fiandaca, Musco, *op. cit*., pagg. 621-679.

[252]*Ibidem.*

[253] Fiandaca, Musco, *Diritto Penale - Parte Speciale*, vol. I, Zanichelli Editore, 1997, pagg. 396 e ss.; Pulitanò, *Il favoreggiamento personale tra diritto e processo penale*, Giuffrè, 1984.

[254]Riportando qui la disposizione della fattispecie:<< Chiunque, dopo che fu commesso un delitto per il quale la legge stabilisce [la pena di morte] l'ergastolo o la reclusione, e fuori dai casi di concorso del medesimo, aiuta taluno a eludere le investigazioni dell'Autorità, o a sottrarsi alle ricerche di questa, è punito con la reclusione fino a quattro anni.>>

[255]Corvi, *op. cit.,* pag. 604.

[256]*Ibidem.* Questo perché<< appare davvero difficile affermare che il senatore fosse gravato da un obbligo di protezione nei confronti della vittima, né , tanto meno, di un obbligo di controllo nei confronti della mafia>>.

[257]*Ibidem.*

quella stessa caratteristica che non considerava bastevole per la configurazione della condotta di partecipazione[258].

Questa commistione di correnti giurisprudenziali, generanti l'adozione di questa corrente<<mista>> (maggiormente adottata sia dalla dottrina e dalla giurisprudenza), ha difatti creato non poche complicazioni sul piano probatorio: da un lato, riguardo l'utilizzo dei medesimi elementi di prova per dimostrare le due diverse caratteristiche costituenti la condotta di partecipazione (ossia, l'inserimento organico e la rilevanza causale della condotta); ma anche dall'altro lato nella resa più gravosa dell'onere probatorio[259].

In chiusura, un ramo della dottrina[260] scorge nei criteri causale e organizzatorio diverse problematiche (e - si aggiunge - da considerare valide anche per quello <<misto>>, dato che esso è la sintesi dei due):

- Affinché il soggetto sia identificato come partecipante, è necessario che, una volta inserito nell'organizzazione ponga per forza in essere un'attività di rilevanza casuale (come il criterio casuale vorrebbe) oppure basta un c.d. <<atto di militanza>>[261]? Detto più semplicemente: il <<soggetto maldestro>>[262], che assume un ruolo nell'associazione e pone compie delle attività dimostranti il suo impegno e l'intenzionalità di contribuire alla vita dell'associazione ma che non sono casualmente rilevanti per la stessa, è sempre da considerare partecipante o no?

- *Quid iuris* nel caso del soggetto che decida di aderire all'associazione, venga accettato come membro dagli associati, assuma un ruolo, ma non compia alcuna attività esecutiva inerente il ruolo stesso? Come indica l'Autore, solo nel caso del <<paradigma 'organizzatorio' puro, […] elaborato dalla giurisprudenza in tema di associazione di tipo mafioso>>[263], si configurerebbe la condanna di partecipazione. Invece, nel caso del criterio causale si escluderebbe l'ipotesi di partecipazione per tutti i criteri utilizzati per l'individuazione della condotta di associazione a delinquere c.d. semplice.

---

[258]È curioso notare chene la conclusione del commento di Corvi si ritrova un punto già sottolineato da De Francesco sul materiale probatorio, visto precedentemente riguardo la descrizione del criterio organizzatorio.
[259]A conferma di quanto detto, si riprende la preoccupazione di : De Francesco, *op. cit.*, pag. 145, che indica come la costante simmetria tra la condotta di partecipazione e lo <<svolgimento di attività materiali specifiche>>rende sempre più sfumate le diversità tra la responsabilità penale per l'associazione a delinquere in quanto tale e quella per le singole attività volte a perseguire la consumazione dei delitti-scopo.
[260]Viganò, *op. cit*., pagg. 315-7.
[261]*Ivi,* pag. 315.
[262]*Ibidem.*
[263]*Ivi,* pag. 316. Senza andare nel dettaglio, si fa riferimento all'assunzione della qualifica come <<uomo d'onore>> tramite un apposito rito posto dall'associazione mafiosa. Per maggiori dettagli, si fa riferimento a : Tona, *op. cit*., pag. 1108.

In sintesi,questa costante oscillazione tra l'elemento casuale del contributo e l'inserimento organizzativo come requisiti della condotta di partecipazione non solo crea non poche problematiche sul piano probatorio, ma rende arduo trovare una definizione di partecipazione che non sfoci nella mera disponibilità ad associarsi (come è stato, ad esempio, nel commento della sentenza della Cassazione visto precedentemente[264]).

Seppur si comprenda l'esigenza politico-criminale di punire questi fenomeni associativi, viene evidenziato come questo continuo riallacciarsi alla mera disponibilità rischi di rendere penalmente perseguibile solo la <<mera intenzione di agire>> e non piuttosto <<il fatto dell'avvenuto incardinamento nell'organizzazione>>[265], facendo quindi perdere la dimensione della pericolosità ed offensività dell'associazione.

3.2. Brevi cenni sull'elemento soggettivo del reato.

Al fine di conferire maggior completezza al lavoro svolto finora, non si può chiudere l'analisi dell'associazione a delinquere semplice senza fare una breve disamina anche dell'elemento soggettivo del reato.

Il delitto in esame richiede il dolo, consistente - in riferimento specifico alla fattispecie in esame- nella coscienza e volontà della condotta di partecipante (semplice o qualificata che sia). Tuttavia, affinché si configuri l'elemento soggettivo nella fattispecie in esame, il mero dolo non basta: è anche necessaria l'ulteriore presenza sia della consapevolezza del partecipante di contribuire << in modo stabile e permanente al sodalizio criminoso>>[266] con lo scopo di commettere delitti, ma anche che il soggetto sia a conoscenza del fatto che vi siano almeno altri due soggetti partecipanti alla realizzazione del medesimo programma criminoso [267]. Deve quindi necessariamente sussistere il dolo specifico[268].

[264]Oltre a richiamare quanto detto dall'Autrice nel corso del paragrafo, si rimanda anche a Viganò, *op. cit.,* pag.317.
[265]Viganò, *op. cit.,* pag.317.
[266]Per la dottrina: Fiandaca,Musco, *op. cit.,* pag. 489. Per la giurisprudenza, si veda: Cass. pen., Sez. II, n. 3514113/2019,in *Cass.Pen*. , 2020, fasc.3, pag.1167; Cass. pen. sez. VI , n. 50334/2013, in C.E.D. Cass. pen. 2013; Cass. pen. sez. VI , n. 9117/2011, in C.E.D. Cass. pen., 2011; Cass. pen. sez. VI del 10/05/1994,in *Cass. Pen*., 1996, pag. 1124. *Contra:* Boscarelli, *op. cit.,* pag.4. .
[267]De Francesco, (*voce) Associazione a delinquere e associazione a delinquere di tipo mafioso*, pag. 303. Nello stesso senso:Insolera, *op. cit*., pag. 228, Consulich, *op. cit*, pag. 120.

Tuttavia, bisogna fare alcune apposite precisazioni:

- Tutte le figure di partecipanti qualificati devono avere ulteriormente la consapevolezza dell'esistenza della loro qualifica e la volontà di esercitarla[269];
- ai fini della configurazione del dolo specifico, per il promotore si esclude la conoscenza dell'esistenza di almeno altri due soggetti facenti parte del sodalizio. Questo perché questa figura di partecipazione agisce prima ancora che venga posta in essere l'associazione: perciò, in riferimento a quest'ultimo si deve piuttosto verificare la presenza di <<una contemporanea presenza di altri soggetti concorrenti con il promotore [….] alla creazione di un ente>>[270].

Non è invece necessario che il partecipante abbia conoscenza di chi siano effettivamente i membri[271]. Inoltre, è irrilevante quale sia il motivo per cui egli aderisce e partecipa all'associazione o se egli abbia partecipato tramite mandato di terzi[272].

Si deve segnalare che la rilevazione del dolo specifico è per la giurisprudenza un fondamentale punto di partenza. Infatti, da esso non solo si può individuare se il soggetto è responsabile per condotta di partecipazione semplice o per una delle condotte di partecipazione qualificata, ma da esso si può arrivare alla dimostrazione della stessa esistenza dell'associazione a delinquere: questo però solo se l' <<attività conforme al piano associativo>>[273]sia stata un'attività costante (ossia se, dalle modalità esecutive del partecipante e da altri elementi indiziari emerga una certa <<continuità, frequenza ed intensità dei rapporti degli associati>>)[274]. Anche nel caso in cui il soggetto abbia preso parte alla realizzazione di un singolo delitto-scopo, si può arrivare alla dimostrazione della sua appartenenza all'associazione a delinquere: tuttavia, questo mero indizio deve esser puntualmente sostenuto da ulteriore ed adeguato materiale probatorio[275].

---

[268]Proprio perché l'elemento soggettivo nell'art. 416 c.p. ha come requisito il dolo specifico, si deve necessariamente escludere la realizzazione di concorso di dolo eventuale (Cass. pen. sez. II n. 4342/1994, in CED Cass. pen. 1994).

[269]Cavaliere, *Associazione per delinquere,* in Moccia (a cura di), *Trattato di diritto penale. Parte speciale*, vol.V - *Delitti contro l'ordine pubblico*, Edizioni scientifiche italiane, 2007, pag. 310. Nello stesso senso: Borsari, Provolo, *op. cit*., pag. 48.

[270]De Francesco, (*voce) Associazione a delinquere e associazione a delinquere di tipo mafioso*, pag. 303.

[271]Fiandaca,Musco, *op. cit.,* pag. 489.

[272]Tona, *op.cit.*, pag. 1102 . Nello stesso senso: Borsari, Provolo, *op. cit.,* pag. 48. Per la giurisprudenza, si veda: Cass. pen. del n. 33717/2001, in C.E.D. Cass. pen., Rv. 2219921.

[273]Cass. pen., Sez. II, n. 3514113/2019,in *Cass.Pen*. , 2020, fasc.3, pag.1167.

[274]Si fa in particolar modo riferimento a : Cass. pen. sez. VI del 10/05/1994,in *Cass. Pen*., 1996, pag. 1124.

[275]Vedi nota 273).

Bisogna poi menzionare un interessante pensiero che colloca la figura del dolo specifico descritta poc'anzi in una particolare prospettiva: considerato che il dolo specifico consiste nello scopo di commettere più delitti condiviso dai membri appartenenti alla stessa associazione, esso assumerebbe una dimensione di natura collettiva, tale da far rinvenire nello stesso elemento soggettivo del reato in questione <<un risvolto di carattere oggettivo>>[276]. Questa dimensione collettiva del dolo permetterebbe, nel caso in cui vi sia la presenza di un'organizzazione stabile e un programma criminoso dettagliato e preciso, di poter rilevare la presenza del dolo nella mera adesione, senza compiere ulteriori indagini sulla questione.[277]

In realtà, questa visione si presta a delle critiche: come è stato fatto notare da un ramo della dottrina[278], nella prassi è difficile - se non improbabile – che venga individuata e condannata un'associazione a delinquere semplice (ma anche di tipo mafioso) prima ancora che essa commetta i delitti-scopo ovvero che i suoi partecipi abbiano posto in essere <<condotte esterne materialmente rilevabili>>[279]. Quanto detto si collega anche alla tendenza della giurisprudenza, al fine di affermare o escludere la presenza del dolo specifico, di ricercare elementi concreti che consentano di far rilevare la partecipazione attiva dei membri : si è notato[280] come le prove dimostranti la sussistenza del dolo vengano spesso ricercate dalla giurisprudenza non tanto al momento dell'adesione del soggetto all'associazione, ma quando invece il partecipante dimostra un comportamento esterno manifestante la volontà di contribuire al mantenimento e sviluppo della vita dell'associazione[281] .

In chiusura a questo sintetico quadro, ci si deve soffermare sull'esistenza d'un forte legame tra l'elemento soggettivo ed una tematica trattata poc'anzi: la condotta di partecipazione. Se nel processo dimostrare l'esistenza del dolo specifico dipende strettamente dagli elementi di prova dimostranti <<l'appartenenza al sodalizio>>[282], l'individuazione d'un criterio della partecipazione accolto unanimemente da dottrina e giurisprudenza ed in grado di tenere conto delle esigenze di elementi concreti date dalla prassi , renderà molto più agevole l'attività d'individuazione dell'elemento soggettivo nella fattispecie concreta.

---

[276]Patalano, *op. cit*., pag. 98.
[277]*Ibidem.*
[278]Tona, *op .cit*., pag. 1103.
[279]*Ibidem.*
[280]*Ivi,* pag. 1104.
[281]Cass. pen. n. 6239/1999, in C.E.D. Cassazione penale, Rv.212810.
[282]Tona, *op.cit*., pag. 1105.

Infine, è corretto segnalare che un cospicuo ramo della dottrina ammette l'esclusione del dolo in presenza di ignoranza dell'illiceità del programma [283] .

3.3. La configurabilità del concorrente esterno nella fattispecie associativa

Nonostante spesso lo studio della fattispecie di concorso si sviluppi in via molto più frequente con riguardo alle associazioni a delinquere di tipo mafioso che rispetto a quelle semplici, è comunque doveroso concludere aprendo una piccola parentesi su quest'argomento, poiché - come ben si vedrà lungo la sua trattazione,in realtà sono presenti molti più legami di quello che si andrebbe a pensare.

Innanzitutto, bisogna menzionare che il concorso di persone ex art. 110 c.p.[284] prevede la punibilità per tutti quei soggetti che insieme commettono un reato doloso, e che è una clausola generale, nel senso che prevede la punibilità dei concorrenti, senza alcuna distinzione tra le modalità di partecipazione dei diversi concorrenti[285].

È dunque reso evidente come possa essere nella pratica arduo distinguere se si tratta di un'associazione a delinquere o di un concorso eventuale di persone(specie se il disegno criminoso di queste ultime è particolarmente complesso e riguarda più delitti).[286] Nella ricerca di una soluzione alla problematica, si trovano due principali criteri utilizzati per la loro distinzione:

1. Un ramo corposo della giurisprudenza e della dottrina[287] individua l'elemento distintivo tra il delitto di associazione per delinquere e il concorso di persone nel reato ex art. 110 c.p. nella stessa natura dell'accordo. Nel caso dell'art.416 c.p., la commissione di uno o più reati-scopo non fa minimamente venir meno l'accordo: questo, proprio per la presenza d'un vincolo associativo stabile avente come obiettivo la commissione di una serie

[283]Boscarelli, *op. cit*., pag. 3.Nello steso senso: Fiandaca, Musco, *op. cit*., pag. 489; Borsari, Provolo, pag. 48.V. anche: De Francesco, *op. cit*., pag. 306.
[284]Riportando qui la disposizione della fattispecie: <<Quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita, salve le disposizioni degli articoli seguenti>>.
[285]Si fa riferimento a : Fiandaca, Musco, *op. cit*., pag. 523 e ss.
[286]Misaggi, *op. cit*., pag. 89.
[287] Per la dottrina, si cita: Consulich, *op. cit.,* pag. 116; Burzi*, Nota sui requisiti per la sussistenza del reato di associazione per delinquere* (nota alla sentenza Cass. Pen., Sez. I n. 39757/2005) in *Giur. It.*, fascicolo 7/2006, pag. 1485. Per la giurisprudenza,si cita: Cass. pen. sez. V , n. 1964/2018, in C.E.D. Cass. Pen. 2019; Cass. pen. sez. III n. 11570/2020, in *Responsabilità Civile e Previdenza,* 2020, Vol.4, pag. 1305.

indeterminata di reati-scopo (a prescindere che siano poi effettivamente commessi o meno);

Oltre alla stabilità del vincolo associativo, vi è una corposa parte della giurisprudenza e dottrina che considera l'elemento dell'indeterminatezza del programma al fine di distinguere l'associazione a delinquere rispetto al concorso di persone ex art. 110 c.p. Nello specifico, per indeterminatezza del programma si fa chiaro riferimento << […] al numero, alle modalità, ai tempi e agli obiettivi dei delitti programmati, i quali, invece, devono essere di per sé ben individuabili nel genere e nella specie>>[288].

Partendo dalla dottrina, un primo pensiero [289]specifica come per distinguere l'associazione per delinquere dal concorso di persone nel reato continuato non basti il requisito dell'organizzazione, perché esso compare anche nel concorso come <<elemento di rafforzamento del sodalizio criminoso>> [290]; così come il numero di delitti e la caratteristica della permanenza dell'organizzazione. Ciò che permette davvero di tracciare il confine tra le due figure di reato sarebbe piuttosto l'indeterminatezza del disegno e dell'esecuzione dei delitti: questa caratteristica, propria solo dell'art.416 c.p., creerebbe già un pericolo per l'ordine pubblico, rendendo punibile il vincolo associativo. Invece, <<l'associarsi per commettere un determinato delitto, costituisce […] un atto preparatorio, che sfugge alle sanzioni del codice penale>>[291].

Altra posizione, arrivando sempre alla conclusione che ciò che contraddistingue l'art. 416 c.p. è la stessa genericità del programma delittuoso, osserva in particolare come l'associazione , a differenza del concorso[292], sia <<una riunione stabile di più persone legatesi tra loro col proponimento di delinquere e mirante all'attuazione di un programma criminoso in cui la specificazione di delitti può essere anche omessa, come può mancare l'esecuzione di essi>>[293].

Infine, si segnala che questa differenza comporta un impatto anche sul piano soggettivo: per il fatto che i soggetti partecipano alla realizzazione di un programma indeterminato, ne

[288]Per questa definizione Misaggi, *op. cit*., pag. 89, fa riferimento a: Boscarelli, *op. cit*., pag. 869.
[289]Marciano*, Associazione pre delinquere e concorso criminoso,* in Id*., Questioni di diritto- con note di Enrico Altavilla,* Morano, 1926.
[290]Marciano*, op. cit.,* pagg. 265.
[291]Marciano*, op. cit.,* pagg. 265-266.
[292]Nello stesso senso:De Francesco, *(voce) Associazione per delinquere e associazione di tipo mafioso,* pag. 292, il quale precisa come la stessa indeterminatezza e genericità del programma conferisca <<entità autonoma>> rispetto alla preparazione dei delitti-scopo.
[293]Salerno,*Concorso delittuoso e associazione a delinquere* , in *Scuola Pos*., Vol. I, 1930, pag.54.

fa conseguire la presenza dell'intenzione di distribuirsi anticipatamente i ruoli tra i partecipanti per la commissione dei delitti-scopo, << "pensati" in chiave di caratteri strutturali permanenti del vincolo associativo>>[294].

Per quanto riguarda la posizione della giurisprudenza, s'identifica come molto spesso, quando vi sono più condotte delittuose, si commetta l'errore di considerare immediatamente l'applicazione dell'art. 416 c.p. senza aver controllato se vi sia la presenza di un programma delittuoso indeterminato.

Questo in particolare emerge da una sentenza della Corte d'Appello di Roma del 2016[295], dove i giudici hanno escluso che nella vicenda in esame si applicasse l'art. 416 c.p.. Secondo il loro ragionamento, seppur vi fossero le prove che <<l'attività continuativa di appropriazione del denaro del partito è stata oggetto di un ben congegnato sistema criminoso, non occasionale o contingente>>[296]; mancava la prova che quell'accordo facesse parte di un più generale programma, capace di durare anche dopo il perseguimento di quell'obiettivo accertato.

Da questa sentenza emergerebbe dunque come, nell'ipotesi di più condotte illecite coinvolgenti più persone, non si può parlare di associazione per delinquere se l'accordo sia finalizzato solo a realizzare uno specifico scopo criminoso e non anche a dar vita a un vincolo stabile,<<perdurante anche dopo l'esaurimento della serie di reati programmata ex ante>>[297].

---

[294]De Francesco, *op. cit.*,pag. 291. Questo anche spiega perché Id., a pag. 507, esegue un'ulteriore distinzione tra il concorrente esterno (rispetto al partecipante sul profilo oggettivo. Infatti, al concorrente risulterebbe mancare <<il dato psichico, consistente […] nel sentirsi parte insieme ad altri di un'istituzione, di identificare i propri scopi […] in quelli del sodalizio.>>[294](Patalano, *op. cit.,* pag. 227). Difatti, il concorrente esterno non agisce per commettere i delitti previsti nel programma; quanto preferibilmente più con l'intenzione di contribuire saltuariamente e con l'obiettivo che le sue attività non siano ricollegabili all'associazione. Un esempio citato è quello della dattilografa che scrive delle lettere minatorie per conto dell'associazione a delinquere che ha come obiettivo l'estorsione di denaro a famiglie ricche: in questo caso, <<la consapevolezza di agire per conto di un sodalizio criminoso, agevolandone l'attività>>, non è la partecipazione all'associazione, perché la dattilografa rimane comunque al di fuori dell'associazione.

[295]App. di Roma, Sez. III, n. 2984/2016. Il caso era relativo ad una serie di operazioni finanziarie finalizzate esclusivamente a sottrarre risorse economiche ad un noto partito politico italiano.

[296]Cfr. App. di Roma, Sez. III, n. 2984/2016.

[297]Miglio, *Brevi appunti in merito alla necessaria distinzione tra associazione a delinquere e concorso di persone nel reato continuato*, nota alla sentenza App. di Roma, Sez. III, n. 2984/ 2016), in Giurisprudenza Penale Web, 2016, numero 12, pag.2. L'autore anche accenna al fatto che con quest'impostazione si realizzano non poche ripercussioni di carattere processuale: se vi è un'erronea contestazione del delitto di associazione per delinquere si rischia di creare un inutile allungamento dei tempi del procedimento penale, determinando la prescrizione dei reati-scopo; facendo sì che l'evidente conseguenza che tutte queste condotte illecite che, non necessariamente oggetto di un programma, ma piuttosto di un puntuale disegno criminoso, <<rimangano – di fatto – impunite>>.

Spostandosi adesso sulla figura del concorrente esterno, parrebbe possibile in tutte le fattispecie a concorso necessario (art. 416 c.p. compreso[298]) il poter prevedere soggetti diversi dai c.d. concorrenti necessari, purché <<il reato plurisoggettivo, sul quale si innestava il concorso eventuale, fosse completo in tutti i suoi elementi>>[299].

In base dell'art. 110 c.p., il concorrente esterno è il soggetto che (specificamente riguardo le associazioni a delinquere), non fa parte dell'associazione e non ha intenzione di collaborare per perseguire l'intero programma criminoso , ma che <<in via occasionale […] offre aiuto e sostegno con specifiche azioni utili all'ente.>>[300]. Perciò, quello che si cercherà di capire è se davvero si può configurare un concorso esterno nel caso dell'associazione a delinquere semplice (anche sulla base di quanto detto prima sulla partecipazione).

Per lungo periodo vi sono stati pareri contrastanti sul punto, sia in dottrina che in giurisprudenza.

Partendo dalla prima, i pensieri della dottrina divergono a seconda del tipo di criterio da loro accolto per l'individuazione della condotta di partecipazione ex art. 416 c.p.:

- gli studiosi sostenitori del criterio causale per l'individuazione della condotta di partecipazione escludono la configurazione del concorso esterno per le associazioni a delinquere semplici[301]: chiaramente, se il contributo dev'essere causalmente in grado di incrementare il livello di pericolosità dell'associazione a delinquere e deve essere stabile, è ovvio che una condotta di carattere sporadico e non necessariamente avente valore causale rispetto all'incremento della pericolosità dell'organizzazione, non assume alcuna rilevanza penale.

- Invece, per chi adotta il criterio organizzatorio, sarebbe ammissibile la figura del concorrente esterno, poiché si tratterebbe di un <<mero avvicinato>>,[302] quindi un soggetto non avente un vero e proprio ruolo all'interno dell'organizzazione.

---

[298]Si richiama l'introduzione di questo capitolo sull'aspetto della plurisoggettività.

[299] Cass. pen. del 18/03/2004 in *Dir. Pen. e Proc*., 2004, pag. 685. *Contra:* Muscatiello, *op. cit.,* a pag. 165, in cui si menziona che la concorrenza esterna deve consistere << in un apporto *sine quo non* dell'altrui svolgimento stabile e permanente della funzione all'interno del sodalizio- non come semplice aiuto ad un singolo episodio di altrui partecipazione.>>.

[300]Tona, *op. cit*., pag. 1132.

[301] Nello stesso senso: Tona, *op. cit*., pag. 1132. Altro autore a sostegno dell'esclusione del concorrente esterno è: Grosso, *op. cit*., pag. 419.

[302]Tona, *op. cit*. , pag. 1132.

Altro punto fermo accolto da questo ramo dalla dottrina è la precisazione che il soggetto concorre <<all'associazione nel suo complesso, intesa come realtà organizzativa superindividuale, distinta rispetto alle condotte dei singoli partecipi>> [303] e non alla specifica condotta partecipativa (semplice o qualificata che sia): nel secondo caso, si parlerebbe piuttosto di reato di favoreggiamento[304].

Riguardo invece la giurisprudenza, vi sono stati diversi orientamenti sul punto:

- Ovviamente, il ramo della giurisprudenza aderente al modello causale della partecipazione, al pari della dottrina vista sopra, ha negato la sussistenza del concorso esterno[305] ;

- Vi sono altre decisioni [306] che invece, escludono l'ipotesi del concorso esterno per l'associazione a delinquere, salvo alcune ipotesi specifiche (come, ad. es. i casi di istigazione a delinquere, nonché nelle condotte qualificate dell'art. 416 c.p.): infatti, mancherebbe per il concorrente esterno l'elemento dell'*affectio societatis* (cioè <<l'esistenza di un vincolo associativo non circoscritto ad uno o più delitti, ma consapevolmente esteso ad un generico programma delittuoso>>[307]), nonché <<la condotta esprimente l'apporto all'organizzazione già formatasi o mentre si forma>>[308].

- Altro ramo della giurisprudenza[309] ammette invece l'ammissibilità del concorso esterno, ma solo in quanto <<supporto esterno>> [310] , non essendo legato alla struttura dell'associazione;

- Infine, vi è quella posizione della giurisprudenza (più recente)[311] che ammette il concorso esterno, ma alla condizione che sussistano due requisiti: uno è il c.d. <<profilo

---

[303]Viganò, *Riflessioni Conclusive*, in *I reati associativi: paradigmi concettuali e materiale probatorio. Un contributo all'analisi e critica del diritto vivente*, (a cura di) Picotti, Fornasari, Viganò, Melchionda, CEDAM, 2005, pag. 319.

[304] A sostegno di questo punto, si veda, nella giurisprudenza: Cass. pen. sez. III n. 47436/2021, in *Guida al diritto* 2022, vol. 7; Cass. pen. sez. I del 13/06/1987 in *Cass. Pen*. 1988, pag. 1812. Cass. pen. sez. V, n. 33874/2021, in C.E.D. Cass. 2021.

[305]Cass. pen, n. 8864/1989 in *Cass. pen*., 1991, pag. 1042; Cass. pen., cit. ,n. 8092 /1987 in *Cass. pen.,* 1989, pag.36;Cass. pen. sez. I del 18/03/1994 in *Cass. pen*. 1994, pag.2685.

[306] Cass. pen. Sez I del 21/03/1989, in C.E.D. Cass. n.181637.

[307] La definizione si riprende in: Cass. pen., Sez. I del 01/07/1988 in *Giust. Pen*., 1989, Vol. II, pag. 535.

[308]Cass. pen. Sez I del 21/03/1989, in C.E.D. Cass. n.181637.

[309]Cassazione penale sez. I del 24/01/1994, in *Giust. Pen*., 1994, Vol.II, pag.424

[310]Tona, *op. cit.* , pag. 1132.

[311]Cass. pen. Sez. I del 23/11/1992, in *Cass. Pen*., 1995, pag. 45; Cass. pen. Sez. II, n. 47602/2012, Rv. 254105; Cass. pen. sez. VI del 25/06/1999 in *Cass. pen*. 2000, pag.1179.
In particolare, si segnala che nella sentenza Cass. pen. sez. VI del 25/06/1999 emerge anche l'elemento dell'emergenza nella vita associativa: <<Il concorrente esterno deve avere, però, la consapevolezza del

materiale>>[312], ossia la presenza di prestazioni di singoli comportamenti coerenti rispetto allo scopo sociale o per il mantenimento della struttura associativa. Il secondo invece è il profilo psicologico, consistente ne <<la consapevolezza dell'esistenza dell'associazione e la coscienza del contributo che ad essa arreca>>[313].

In ogni caso, nonostante le non poche oscillazioni viste, parrebbe che odiernamente, sia dottrina che giurisprudenza propendano per l'ammissibilità del concorso esterno[314] nella fattispecie.

Tuttavia, la questione più problematica riguarda l'individuazione delle differenze tra la condotta di partecipazione ed il concorso esterno ex art. 110 c.p.[315]: questo perché, come indicato da Tona, *ibidem,* a pagina 1134, sono entrambe condotte a forma libera[316].

Sebbene questo sia un argomento molto ampio, si cercherà comunque di fare qualche richiamando due interessanti riflessioni sul tema.

1. Tendenzialmente, si tende a considerare come concorrente eventuale il soggetto che pone in essere <<*qualsiasi* condotta che apporti un *contributo causale* all'associazione stessa […]>>[317]. A questo però fa immediato seguito una domanda: è proprio necessario che vi sia un contributo casuale della condotta del concorrente esterno per il rafforzamento dell'associazione? Vi è infatti il pericolo che il giudice, compiendo un ragionamento controfattuale volto a dimostrare che il contributo sia stato << in concreto ed ex post, utile per l'associazione, […]>>[318], non consideri punibili tutte quelle condotte che non sono state utili per l'associazione.
   In aggiunta, s'osserva che, negli articoli 416 c.p. e 110 c.p. , vi sono requisiti diversi per la condotta di partecipazione ed il concorso esterno: se per la prima si tratterebbe di un reato di mera condotta; non vi sono dubbi che invece il concorso nel reato sia un reato

---

"valore" del suo contributo, nel senso che deve rendersi conto che la sua azione, al di là del fine personale perseguito, va a risolvere "problemi e difficoltà" di un sodalizio criminoso di cui ben conosce l'esistenza, […] >>. Nello stesso senso: Cass. pen. sez. V, n. 33874/2021, in C.E.D. Cassazione 2021.

[312]Tona, *op. cit*., pag.1133.

[313]Cass. pen. Sez. II, 29- 11-2012, n. 47602 , Rv. 254105.

[314]Per la dottrina, si trova, a sostegno di questa posizione: De Francesco, (voce) *Associazione per delinquere e associazione di tipo mafioso*,pag. 506; Viganò , *op. cit.,* pag. 319; Muscatiello, *op. cit*., pagg. 132-147; Lattanzi, *op. cit.,* pag. 76; Tona, *op. cit.*, pagg. 1133-1134. *Contra*: Grosso, *op. cit*., pag. 419.
Per la giurisprudenza, si rimanda al ramo più recente della giurisprudenza summenzionato.

[315] Su questo punto concordano: Marinucci in *Conclusioni* ne *I reati associativi ,* (a cura di) Ministero di grazia e giustizia, Fondazione Centro internazionale su diritto e società ed economia, Courmayeur; 1998, Giuffrè, pag. 299; De Francesco, *(voce) Associazione per delinquere e di tipo mafioso,* pag. 305 Lo stesso De Francesco in *Societas Sceleris*, a pag. 147, accennava al <<rischio di considerare membro del sodalizio anche il concorrente meramente <<eventuale>>, non soltanto nel reato associativo>>.

[316]Per la definizione, si richiama al punto a) di questo paragrafo.

[317]Viganò, *op. cit*., pag. 319.

[318]*Ivi,* pag. 321.

d'evento. Di conseguenza, per il concorrente si dovrà dimostrare necessariamente che, senza la sua condotta, il reato non si sarebbe compiuto (o perlomeno, con tempi o con modalità esecutive diverse): un fatto, secondo l'Autore, insuperabile persino per <<il potere 'creativo' della giurisprudenza>>[319].

2. Ultimo ragionamento da affrontare - ma non meno importante - è quello di porsi l'arduo compito d'individuare gli elementi distintivi tra la condotta di partecipazione nell'associazione a delinquere semplice ed il concorso eventuale[320]. Più precisamente: come si deve considerare la posizione del soggetto, il quale presti un contributo all'associazione nel suo complesso, pur in mancanza di un vero e proprio vincolo associativo?

   In realtà, nonostante ancora non si riesca a trovare una specifica risposta a questa domanda, è stata rilevata la tendenza nel voler necessariamente considerare qualsiasi condotta diversa da quella <<dell'essere *socius* >>[321] e automaticamente inquadrarla nel concorso esterno in quanto egualmente meritevole di sanzione penale.

   Di fronte a questa situazione, non bisognerebbe cercare soluzioni volte a rendere penalmente perseguibili ad ogni costo tutte quelle condotte che presentano alcune o quasi tutte le caratteristiche della partecipazione. Il giurista piuttosto dovrebbe controllare*, in primis*, se la condotta in questione - sulla base della disciplina di concorso di persone nel reato- <<influisca sulla realizzazione di quella tipica ovvero contribuisca alla realizzazione dell'evento naturalistico se, ed in quanto, normativamente configurato>>[322].

Quanto detto finora dimostra che in realtà la questione di distinzione tra le due condotte rimarrebbe ancora irrisolta: se, di fatto, non è possibile nell'attività interpretativa trovare una distinzione netta ed incontrovertibile delle due condotte; l'interprete a maggior ragione

---

[319]*Ivi,* pag. 322.

[320]Bertorotta, *Concorso eventuale di presone e reati associativi,* in *Riv. It. di Dir. e Proc. Pen.,* 1998,fasc.4, pagg. 1288-1289, pone, al fine di eseguire più agevolmente il ragionamento, la distinzione tra una << nozione ristretta>> ed una << nozione allargata di partecipazione>>:

- Con la nozione ristretta si guarderebbe alla considerazione che, affinché la condotta venga qualificata come di partecipazione semplice ex art. 416 c.p. è necessaria, oltre al contributo materiale, <<la concreta integrazione>>della c.d. *affectio societatis*;
- Nel secondo caso si andrebbe piuttosto a configurare come partecipazione qualsiasi contributo volontario fornito all'associazione, <<indipendentemente da un effettivo inserimento del soggetto attivo nell'organizzazione criminale, e da un'assegnazione di ruoli e funzioni>>[320].

[321]*Ibidem.*

[322]Bertorotta, *op. cit*., pag. 1291

è ancor di più in un'ardua impresa quando si ritrova a dover comprendere quale delle due norme applicare rispetto la fattispecie concreta.

In conclusione, la consistente dottrina e giurisprudenza che tuttora continuano a discutere sulla compatibilità e sui limiti di queste due diverse condotte, è forse un segnale rivelatore che la condotta del concorrente esterno nel caso della fattispecie associativa semplice è profondamente legata ad essa[323].

Inoltre, emerge un aspetto da non trascurare: se davvero il concorso eventuale venisse usato come mero strumento per estendere l'applicazione della norma anche a condotte atipiche[324], questo sarebbe un altro elemento a sostegno della necessità di revisione degli elementi caratterizzanti la partecipazione, considerando anche le nuove dimensioni delle associazioni a delinquere e le diverse modalità in cui si può configurare la partecipazione.

Una volta definiti i contorni della partecipazione sarà più facile individuarla nelle situazioni concrete, e - di conseguenza - sarà forse possibile trovare una risposta alle domande che ci si è posti lungo il corso di questo sottoparagrafo.

4. Le proposte di riforma dell'art 416 c.p.

In questa prima parte si è voluto investigare sui diversi elementi costitutivi della fattispecie penale, e si è trovato un punto onnipresente alla fine della trattazione di ogni elemento,ossia la necessità che questa fattispecie venga sottoposta all'attenzione del Legislatore, in prospettiva *de iure condendo*: soprattutto, tra le varie ragioni, allo scopo di porre rimedio alla carenza di tassatività della fattispecie, problema strettamente legato alla vaghezza del concetto di associazione e all'inafferrabilità della nozione d'ordine pubblico .

Come già indicato lungo il corso di tutta questa disamina, si deve rintracciare alla base di tutto ciò una scelta di politica criminale nel non specificare eccessivamente gli elementi costitutivi della fattispecie, preferendo lasciarla<<elastica>>, in modo da potere rendere penalmente perseguibili anche le diverse tipologie di associazioni a delinquere emergenti nel futuro.

[323]A sostegno di questo pensiero, si cita: Muscatiello, *op. cit.,* pag. 162, che identifica le due condotte legate da una sorta di <<proprietà commutativa:alla permanenza della partecipazione nel sodalizio fa da *pendant* la permanenza, della natura o dell'efficienza dell'attività concorsuale esterna>>.
[324]Si fa riferimento a quanto affermato da: Bertorotta, *op. cit*., pag. 1293.

Lungi dal voler porre una critica a questa scelta; ma i numerosi dubbi interpretativi emersi durante l'analisi dei diversi elementi della fattispecie penale finora eseguita, potrebbero far sorgere domande più che lecite: oggi, come potrebbe intervenire il Legislatore rispetto alla formulazione dell'art. 416 c.p.? O, in alternativa, converrebbe piuttosto creare *ex novo* delle norme disciplinanti diverse tipologie di associazione a delinquere?

Queste domande, in realtà, non sono per nulla nuove: seguendo un ordine cronologico delle opere dei vari autori, in questa trattazione si cercherà di vedere da vicino alcune nuove prospettive presentate dagli studiosi riguardo la fattispecie dell'associazione a delinquere semplice, nell'auspicio di fornire uno spunto di riflessione finale sulla fattispecie penale finora trattata.

A. Partendo dal pensiero di Insolera, l'Autore si è dedicato ampiamente della problematica della carenza di tassatività della fattispecie e della sua adesione al concetto materiale di ordine pubblico[325], quale bene giuridico tutelato. A ciò seguono interessanti riflessioni sugli aspetti della fattispecie su cui l'autore ritiene sia necessario l'intervento del legislatore[326].

   Il primo – forse il più evidente, considerato quanto detto nell'introduzione - è la necessità di una maggiore collaborazione tra il diritto e la materia della criminologia, al fine di trovare delle soluzioni (e non << in mera funzione apologetica e giustificatoria>>[327]) in grado di ammorbidire il netto contrasto tra la scelta del carattere generale del contenuto della fattispecie(in particolare, nei modi e nelle forme in cui si manifesta) e il contesto strettamente empirico in cui si dovrebbe prevedere la sua applicazione[328]; nonché analizzare meglio le nuove figure associative, soffermandosi in particolare sulla tipologia di organizzazione che viene posta in essere e sulle attività legate ad essa.

Un ruolo fondamentale nella ridefinizione dell'art. 416 c.p. è indubbiamente svolto dal bene giuridico tutelato.

---

[325]In questo, si fa richiamo al paragrafo 1, relativo all'ordine pubblico.
[326]Insolera,*op. cit.,* pagg. 305 e ss.
[327]*Ivi,* pag. 309.
[328]Come indicato da : Insolera, *op. cit.,* pag. 308,l'associazione a delinquere è appunto <<un fenomeno che […] si connota naturalisticamente, ed è empiricamente apprezzabile per la sua *antisocialità,*[…] [ovverosia] la capacità di porre in pericolo o compromettere esigenze basilari, proprie di una civile convivenza>>

A tal proposito, Insolera ritiene, come secondo aspetto, che debba esser prevista esplicitamente nella fattispecie dell'associazione a delinquere la realizzazione del pericolo per l'ordine pubblico come evento tipico, considerandolo appunto <<come ulteriore conseguenza della condotta dell'agente [intesa come la formazione del vincolo associativo, N.d.A.] >>[329].

Ciò consentirebbe, infatti, d'evitare l'utilizzo di formule aventi nessi condizionali (es. <<nel caso che dal fatto derivi il pericolo>>), in grado di creare – e aventi già creato – ulteriori problemi interpretativi nella tematica dell'associazione a delinquere in rapporto all'interesse giuridico protetto dalla norma[330].

Si deve ricordare, però, che non solo Insolera accoglie la c.d. nozione di ordine pubblico intesa in senso materiale[331], ma anche non vede il pericolo come conseguenza immediata della formazione del vincolo associativo: risulta esservi come <<fatto intermedio>> tra i due la formazione della struttura organizzativa dell'associazione.

Conseguentemente, bisogna cogliere, come ulteriore spunto di riflessione dell'Autore, che la mera esplicita indicazione del pericolo come evento non sia in realtà sufficiente: un passo ulteriore che dovrebbe fare il Legislatore nella ridefinizione della fattispecie è quello di definire con precisione<<l'evento associazione, da cui ripetere i connotati della condotta tipica>>[332].

Seppur questa scelta comporterebbe una netta restrizione delle situazioni riconducibili all'art. 416 c.p., essa allo stesso tempo presenta due grossi vantaggi:

- Da un lato, agevolerebbe il funzionamento d'un controllo empirico ed oggettivo <<della validità dei parametri oggettivi>>[333]sulla cui base si rileva la presenza del pericolo per l'ordine pubblico stesso,
- Dall'altro lato, renderebbe necessario, affinché si configuri il dolo specifico nella fattispecie, che il partecipante (quanto meno in via eventuale [334]) abbia una rappresentazione fattuale del possibile pericolo per l'ordine pubblico come conseguenza ulteriore alla sua adesione.

---

[329]Insolera, *op. cit.*, pag. 331.

[330]Si fa in particolar modo riferimento all'art. 44 c.p., cit., rinviando, per ulteriori approfondimenti sulle condizioni obiettive di punibilità: Bricola, *Punibilità (condizioni obiettive d*i), cit., in *Noviss. Digesto It*., vol. XIV, 1967, UTET, pag. 593; Nuvolone, *Il sistema del diritto penale*, cit., CEDAM , 1975, pag. 168.

[331]Si rinvia al paragrafo 1 di questo capitolo.

[332]Insolera, *op. cit.*, pag. 332.

[333]*Ibidem.*

[334]*Ibidem.*

In chiusura della disamina del pensiero di Insolera, considerato che l'art. 416 c.p. è nato in riferimento a specifici modelli di associazioni criminali e la sua applicazione si è in seguito estesa a situazioni sempre più vaste, <<fino a confluire in un'area difficilmente discriminabile dall'operare del concorso di persone>>[335]; l'obiettivo da perseguire per l'Autore è quello di riassegnare valore a tutti gli indizi che permettono d'individuare la presenza della criminalità organizzata, e su di essi <<ricalcare, col necessario processo di astrazione, i criteri definitori della fattispecie incriminatrice>>[336]: processo senza dubbio non semplice, ma per l'Autore irrinunciabile per consentire la sistemazione della fattispecie.

B. Uno studio molto più accurato sulle alternative poste davanti al Legislatore riguardo la fattispecie associativa è stato senz'altro eseguito da De Francesco [337] . Avendo riscontrato[338] non poche problematiche nell'art. 416 c.p. - la carenza di tassatività (in particolare, <<sul concetto stesso di associazione>> [339]), la nebulosità dei confini tra l'associazione a delinquere ed il concorso di persone nel reato, la vaghezza della caratteristica dell'indeterminatezza del programma delittuoso[340] e della condotta di mera partecipazione, nonché la fumosità del concetto di ordine pubblico (e la conseguente incapacità della fattispecie <<di esprimere un autonomo contenuto offensivo>>[341]) - egli ricorda che il reato associativo in sé fa parte della c.d. legislazione d'emergenza[342], posta sulla base di scelte contestuali al periodo storico e, di fatto, di carattere incompatibile <<con le linee di una politica criminale razionale e realmente conforme al <<volto>> costituzionale dell'illecito penale>>[343] .

Questa considerazione storica non è eseguita casualmente: la presenza di istituti così radicali rispetto al sistema penale vigente ha inciso di non poco sull'atteggiamento degli studiosi ed operatori del diritto. Prospettandosi appunto la necessità d'un ripensamento

[335]Insolera, *op. cit.*, pag. 317.
[336]*Ivi,* pag. 318.
[337]De Francesco, *op. cit*., pag. 66 e ss.
[338]*Ivi,* pagg.56-66.
[339]*Ivi.,* pag. 59.
[340]Cfr.: Del Corso, *op. cit.*, pag. 623; ma si richiama anche al sottoparagrafo 2.2. di questo capitolo.
[341] De Francesco, *op. cit*., pag. 65.
[342] Per dare una breve definizione, si considera come legislazione d'emergenza quell'insieme di provvedimenti legislativi che, a partire da1974 (i c.d. <<anni di piombo>>), vengono emanati per combattere prima i fenomeni eversivi, poi anche la criminalità organizzata.
[343]Per maggiori approfondimenti sul tema: Fiore, *op. cit.,* pag. 1103.

generale del sistema normativo in vigore[344], vi sono state diverse soluzioni prospettate riguardo la categoria del reato associativo in sé. Infatti, c'è chi ha eseguito uno sforzo interpretativo notevole per adeguare le fattispecie associative più antiche al clima costituzionale in vigore [345]; altri, dall'analisi delle forme più recenti di criminalità organizzata (ad es., il reato d'associazione mafiosa o il reato di associazione a delinquere finalizzata al traffico di stupefacenti), hanno invece trovato in esse una ratio più lucida e misurata rispetto al passato[346].

Da questi due diversi orientamenti si sono in seguito sviluppati diverse prospettive: chi aderisce alla prima tesi tende a preferire la <<totale eliminazione di qualsiasi fattispecie di carattere associativo>>[347], chi invece predilige la seconda è più invogliato a porre diverse fattispecie penali volte a punire il fenomeno associativo, in misura tale da <<rendere più moderno ed efficiente l'apparato repressivo>>[348].

Andando più nel dettaglio, da questi orientamenti sembrerebbero emergere tre diverse tipologie di soluzioni:

1. La prima ipotesi è l'eliminazione totale dei reati di associazione dal sistema penale[349].
   Quest'idea è derivante dalla difficoltà di identificare chiaramente gli elementi <<strutturali del reato associativo>> [350]: chi sostiene questa soluzione è convinto del fatto che il mantenimento di quest'ultimo condurrebbe ad interpretazioni sempre più estensive, arrivando in extremis a considerare penalmente punibili anche gli atti meramente preparatori. In realtà, De Francesco ha evidenziato come chi sostenga questa soluzione si renda conto che la stessa sia impraticabile[351]: guardando il fenomeno socio-criminologico attuale, si possono infatti trovare numerosi esempi di processi (e maxi processi) aventi ad oggetto la repressione penale di associazioni a delinquere altamente pericolose per le

[344]Come indicato dallo stesso Autore, a pag. 81, <<la tendenza del Legislatore a far spesso ricorso a requisiti[…] caratterizzati da un elevato grado di indeterminatezza condurrebbe […] al risultato d'attribuire sempre al giudice il ruolo di definire gli estremi del fatto incriminato>>.

[345]Per ulteriori approfondimenti sul punto: Nuvolone, *Le leggi penali e la Costituzione*,Giuffrè, 1953; Barile, *(voce)Associazione (diritto di),* vol. III, Giuffrè,1958.

[346]Si segnala sul punto: Neppi Modona, *Criminalità organizzata e reati associativi*, pag.115 e ss.

[347]De Francesco, *op. cit*., pag. 68.

[348]*Ibidem.* Nello stesso senso, si veda: Spagnolo, *Criminalità organizzata e reati associativi: problemi e prospettive*, in *Riv. It. Dir. e Proc. Pen*. , 1998, fasc.4, pag.1161. In dettaglio, egli denota che, seppur vi sia la proposta dell'eliminazione delle fattispecie associative, la maggioranza della dottrina risulti propensa a mantenerle.

[349] Mazzuca, *L'origine dei maxiprocessi e le vie del loro superamento*, in *Anatomia del maxiprocesso (Atti del Convegno),* in *Difesa penale*, 1987, n. 16-17, pag. 23 e ss. .

[350]De Francesco, *op. cit*., pag. 82

[351]*Ivi*, pag. 83.

istituzioni, capaci di alterare il funzionamento delle stesse: è quindi evidente l'esigenza di una risposta penale efficace contro questi fenomeni.

Vista dunque la necessaria presenza della fattispecie dell'associazione a delinquere, si è cercato di adottare allora <<soluzioni di compromesso>>, in grado di conciliare quest'esigenza con l'idea di restringerne l'ambito di applicazione.

Una prima soluzione di compromesso può essere il considerare la punibilità dell'associazione solo se vi siano stati atti esecutivi del programma criminoso. In questo modo, l'art. 416 si qualificherebbe – al pari di altri reati associativi- come <<reato a struttura mista>>[352]: L'associazione può esser punita solo se i reati oggetto del programma siano stati realizzati, anche sotto forma di tentativo[353].
Davanti a questa posizione, viene però sollevata dall'Autore un'obiezione tutt'altro che marginale: a prescindere se il membro dell'associazione sia un soggetto qualificato o semplice, come comportarsi nel caso in cui egli non abbia partecipato alla realizzazione del delitto o dei delitti? Se seguisse l'ottica data da questa visione del delitto in esame come reato a<<struttura mista>>, l'associato verrebbe considerato responsabile per il reato a struttura mista solo se siano posti in essere degli atti esecutivi delittuosi, a prescindere se realizzati dall'associato stesso o da altri membri.
Conseguentemente, non solo accogliendo questa accezione le attività esecutive creerebbero una enorme <<condizione di punibilità>>[354], si otterrebbe la possibilità di intervenire sul piano giuridico contro l'associazione solo nella fase esecutiva, anche se essa di per sé è perseguibile penalmente); ma si darebbe vita anche ad un trattamento sanzionatorio identico per due soggetti che andrebbero invece puniti diversamente, in quanto verrebbe prevista l'applicazione della medesima sanzione sia al partecipante all'associazione per delinquere che al concorrente esterno.

L'altra soluzione di compromesso sarebbe quella di considerare penalmente rilevante solo la commissione dei delitti scopo, riducendo l'associazione a <<mera circostanza aggravante speciale di tali delitti>>[355], ossia un semplice elemento accessorio.

---

[352]*Ivi,* pag. 85.
[353]*Ivi,* pag. 84.
[354]*Ivi.,* pag. 86. Per maggiori approfondimenti, si cita: Angioni, *Condizioni di punibilità e principio di colpevolezza*, cit., in *Riv. It. Dir. e Proc. Pen*., 1989, pagg.1440 e ss.
[355]De Francesco, *op. cit*., pag. 84, trova che vi potrebbe esser un richiamo ad un modello già previsto in materia di contrabbando. In questo senso, si cita: Spagnolo*, Dai reati meramente associativi ai reati a*

Anche con questa <<posizione mediana>>, però, c'è un'altra obiezione mossa dall'Autore: in quest'ipotesi verrebbe perseguito penalmente solo chi ha concorso alla realizzazione del reato, non invece chi si ritrova ad avere funzioni <<di direzione o di <<alta>> organizzazione all'interno del sodalizio>> [356]. In altre parole, seguire questa via comporterebbe responsabilità penale solo per i <<personaggi <<minori>>>>[357], lasciando assolutamente impuniti coloro che ricoprono cariche prestigiose all'interno dell'organizzazione.

In aggiunta, è molto difficile dimostrare la partecipazione nel caso i soggetti non siano <<meri>> partecipanti, soprattutto a causa della fitta trama di occultamenti posta ai vertici dell'associazione.

2. Una seconda posizione consiste nella riduzione del numero delle fattispecie associative, al fine sia di <<evitare incongrue sovrapposizioni […]>> della responsabilità penale, ma anche allo scopo di limitare più possibile il fenomeno dei maxiprocessi[358].

3. Infine,l'ultima ipotesi troverebbe un punto di compromesso tra le precedenti: si penserebbe ad una contemporanea riduzione del numero dei reati associativi ed un intervento sulla struttura dell'associazione, in modo tale da rendere palese il <<disvalore offensivo>>[359]. Con questa prospettiva è necessaria la creazione di fattispecie penali autonome, corrispondenti a<<fenomeni meritevoli di una risposta penale>> [360]. Per far ciò, è chiaramente richiesto uno sforzo consistente di razionalizzazione, anche sotto il profilo politico-criminale.

   Riguardo l'idea di restringimento delle tipologie di associazione a delinquere (e, ulteriormente, gli scopi riconducibili ai reati associativi), è necessario segnalare a tal proposito due orientamenti dottrinali.

---

struttura mista, in AA. VV., *Beni e tecniche della tutela penale,*(a cura di) Crs - Sezione politica e istituzioni in Europa, Franco Angeli Libri, 1987, pag. 156 e ss.

[356]De Francesco, *op. cit*., pag. 85.

[357]*Ibidem.*

[358] Neppi Modona, *Il processo cumulativo nel nuovo codice di procedura penale*, in *Cass. pen*., 1988.

[359] De Francesco, *op. cit*., pag. 79, cita: Insolera, *Sulle diverse forme di criminalità organizzata*, in A.A.V. V., *Beni e tecniche della tutela privata*, Angeli, 1986.

[360] De Francesco, *op. cit*., pag. 80.

Un primo orientamento prende in considerazione l'opportunità di prevedere tante fattispecie di associazioni a delinquere quante sono le tipologie di delitti-scopo rientranti nel programma criminoso, con l'intenzione di <<introdurre un più stretto collegamento tra la struttura dell'associazione e le singole tipologie dei delitti-scopo>>[361].

Oltre ad esser una soluzione molto complessa da attuare nella pratica, essa si presta ad una critica di carattere politico-criminale: oggi difficilmente vi sono associazioni a delinquere perseguenti un programma delittuoso omogenee. Piuttosto, sono sempre più diffuse le associazioni che realizzano delitti diversi, legati <<da una serie di rapporti <<strumentali>>, da un nesso di <<funzionalità>>reciproca tra i singoli obiettivi di volta in volta perseguiti>>[362].

Seguendo questa tesi di selezione delle fattispecie sulla base dei delitti-scopo, si realizzerebbe perciò la presenza di un concorso di diversi delitti-scopo - seppur comunque riconducibili ad un'unica associazione: soluzione - a detta dell'Autore- del tutto sconsigliata, considerando che in questo modo si farebbe darebbe al concorso di reato << il ruolo di una disciplina <<regolare>>>>[363].

Una seconda proposta invece, prendendo ispirazione dall'art. 248 del Codice Zanardelli, propende piuttosto perla previsione di una norma generale dell'associazione a delinquere, ma che sia volta a punirla solo quando essa <<si proponga di commettere reati caratterizzati da un accentuato disvalore offensivo o […] destinati a rappresentare più […] plausibilmente gli scopi di un'organizzazione delittuosa>> [364] . Tutto ciò è posto evidentemente allo scopo di metter freno alla tendenza- conseguente all'estremizzazione dell'anticipazione della tutela penale- di ricondurre all'art. 416 condotte di natura preparatoria.

La ratio nell'Ottocento dietro l'art. 248 era quella di evitare che, lasciando eccessivamente indefinite le tipologie di delitti oggetto del programma, si arrivasse a punire anche quelle

[361] *Ivi*, pag. 129.A sostegno di quest'orientamento parrebbe esserci: De Vero, *Tutela penale dell'ordine pubblico. Itinerari ed esiti di una verifica dogmatica e politico-criminale,* Giuffrè, 1988,pagg. 266 e 267, il quale ritiene che, accogliendo quest'ipotesi si avrebbe il vantaggio di invogliare il Legislatore ad una maggior precisione nella definizione degli elementi dell'art.416 c.p.in relazione ai diversi fenomeni di crimine organizzato manifestatisi nella realtà.
[362] De Francesco*, op. cit*., pag. 130.
[363] *Ibidem*.
[364] *Ivi*, pag. 132. Nello stesso senso: Insolera, *op. cit*., pag. 322.

associazioni non aventi alcun fine delittuoso[365] - anche perché, ai tempi, non veniva riconosciuta ampiamente la libertà di associazione.

Come correttamente sottolineato da De Francesco[366], queste preoccupazioni non hanno però più motivo di esistere, grazie all'art. 18 della Costituzione: se è garantita la libertà di associazione << per fini che non sono vietati ai singoli dalla legge penale>>[367], non possono allora esserci dubbi nell'interpretare l'espressione <<delitti>> in senso letterale (<<tale da implicare,cioè, in ogni caso quel rapporto di corrispondenza con una specifica << legge penale>>>>[368]).

Giunti a questo punto, l'Autore si chiede se sia davvero possibile limitare il campo dei delitti-scopo oggetto del programma criminoso. In realtà, egli è non è tanto convinto di questa tesi: dato che questa soluzione sembrerebbe aver l'obiettivo di escludere tutte le condotte non rientranti nella fase esecutiva del programma,essa<< risente della tendenza di voler identificare l'associazione con un'attività meramente preparatoria>>[369].

Piuttosto, converrebbe portare la fattispecie su un piano più concreto e significativo, <<sottolineandone il carattere di struttura organizzativa potenzialmente permanente>>[370].

Tenendo conto di come si registri una frequenza attuale delle associazioni a commettere delitti contro il patrimonio, contro la persona o delitti di natura politica, De Francesco[371] deduce che:

- Se si vuole davvero selezionare il numero di reati associativi, bisogna imprescindibilmente partire dall'elemento organizzativo, senza il quale vi sarebbero solo i tratti di un mero accordo a commettere più delitti e non un' associazione a delinquere semplice,
- L'idea di eseguire la stesura di diverse fattispecie penali incentrandosi solo sulla tipologia dei delitti-scopo commessi dall'associazione, trascurerebbe non solo gli elementi oggettivi dell'organizzazione, ma anche quegli elementi che permettono di distinguerla dalle attività meramente preparatorie dei delitti-scopo.

---

[365]Si cita, per maggiori approfondimenti sul tema: Cheli, *Libertà di associazione e poteri di polizia: profili storici*, in *La pubblica sicurezza,* (a cura di) Barile, Casa editrice Neri Pozza, 1967, pag. 275 e ss.
[366]De Francesco*, op. cit*., pag. 134.
[367]Art. 18[1] Cost.
[368]De Francesco*, op. cit*., pag. 134.
[369]*Ivi,* pag. 135.
[370]*Ibidem*. Si vedrà, nelle pag. seguenti, la critica posta da Spagnolo sul punto.
[371]*Ivi,*pagg. 136-137.

Tirando le fila del discorso, l'Autore conclude che in una futura configurazione dell'art. 416 c.p. non bisognerebbe tanto interrogarsi su quali delitti possono rientrare negli scopi nel programma criminoso, ma invece <<domandarsi se possano considerarsi compatibili con gli attuali principi costituzionali e con le più recenti tendenze della politica criminale>>[372] le ratio incriminatrici delle fattispecie dei delitti-scopo.

Qualora si decidesse di introdurre nuovi reati associativi, sarà prerogativa essenziale quella di delimitare <<le tecniche di tutela <<anticipata>> rispetto all'effettiva realizzazione dei comportamenti corrispondenti alle relative norme incriminatrici >>[373].

C. Un'ultima riflessione da tenere in considerazione è quella di Spagnolo[374].

L'Autore, prima d'avventurarsi nel delineare le possibili ipotesi di riforma della fattispecie, introduce la questione enunciando che quello delle associazioni a delinquere è un tema che non deve esser più ignorato dal legislatore: bisogna appunto considerare anche come la globalizzazione abbia dato una forte spinta alla criminalità organizzata transnazionale (specie riguardo ai crimini economici) – vista la tendenza in crescita delle alleanze tra diverse associazioni transnazionali, in grado di rendere <<la criminalità individuale […] destinata ad un ruolo sempre più marginale >>[375].

In realtà l'Autore è a sostegno dell'idea che bisognerebbe innovare la fattispecie del reato associativo piuttosto che rimuoverla dal sistema, <<coniugando- per quanto è possibile- garanzie individuali e difesa della collettività>>[376].

Affinché si realizzi ciò, è necessario che nella riforma della fattispecie si proceda contemporaneamente in due direzioni:

---

[372] *Ibidem.*

[373] De Francesco, *op cit.* pag. 137.

[374] Spagnolo,*Criminalità organizzata e reati associativi: problemi e prospettive*, in *Riv. It. dir. e Proc. Pen*., 1998, fasc.4, pag. 1161 e ss.

[375] Spagnolo, *op. cit.,*pag. 1162. Per ulteriori approfondimenti sulla tematica del crimine organizzato in ambito sovranazionale, si cita: Balsamo, Mattarella, Tartaglia, *La Convenzione di Palermo: il futuro della lotta della criminalità organizzata transazionale,* Giappichelli Editore, 2020; Ponti, *Il diritto internazionale e la criminalità organizzata*, in *Rivista di Studi e ricerche sulla criminalità organizzata,* 2015, vol.1, pagg. 23-36; Riondato, *Diritto dell'unione Europea e criminalità organizzata,* in*Reati contro l'ordine pubblico* (a cura di) Fornasari e Riondato, Giappichelli Editore, 2017, pag. 13 e ss.; Vilasi, *La strategia dell'Unione Europea per la lotta alla criminalità organizzata:la centralità dell'informazione e le prospettive di riforma futura,* in *Rivista di Studi e ricerche sulla criminalità organizzata,* 2021, Vol.7.

[376] Spagnolo, *op. cit.,*pagg. 1162 e 1163.

a) <<Arricchire […] la tipicità delle fattispecie associative>>[377], specialmente precisando gli elementi oggettivi,
b) Far sì che le diverse fattispecie associative abbiano un ambito ben delimitato e siano distinte tra loro[378], in modo da evitare la punibilità di associazioni aventi come scopo la realizzazione di delitti di non particolare gravità.

a) Focalizzandosi sulla prima direzione, sarebbe possibile scegliere tra due diverse alternative per raggiungere l'obiettivo di precisare ulteriormente il fatto tipico dell'art. 416 c.p. .

Una prima tesi è quella d'indicare espressamente nella fattispecie dell'associazione a delinquere la presenza di un'organizzazione di carattere stabile[379]. Seppur Spagnolo riconosca che in questo modo si evidenzia l'importanza dell'elemento organizzativo per la realizzazione del fatto tipico dell'associazione, egli non può non esprimere qualche critica su questa posizione: considerato l'incerto andamento giurisprudenziale sulla stessa nozione di organizzazione[380], l'Autore nota come spesso, basandosi solo sull'aspetto dell'<<organizzazione rudimentale>>, giudici e pubblici ministeri tendano a minimizzare il dato organizzativo, evitando<<ogni indagine finalizzata ad accertare la struttura organizzativa anche quando tale accertamento sarebbe agevole>>[381].

Un'altra possibile via d'uscita potrebbe essere quella di prospettata da: prevedere espressamente il requisito dell'adeguatezza alla realizzazione del programma criminoso per la corretta individuazione dell'elemento organizzativo[382], così da chiedere al giudice una costante verifica dell'adeguatezza in ogni processo.

Ma anche quest'ipotesi secondo Spagnolo[383] presenta delle difficoltà, sia sul piano processuale che probatorio: se fosse necessario dimostrare l'adeguatezza dell'organizzazione in sede processuale, di conseguenza la difesa dovrebbe dimostrare in tutti i modi possibili la non adeguatezza dell'organizzazione per la realizzazione del

[377] *Ivi,* pag. 1163.
[378] Lo stesso Autore, in: *Reati Associativi: Prospettive di riforma*, in: Italia Ministero di grazia e giustizia,& Fondazione Centro internazionale su diritto società ed economia, *I reati associativi*. Giuffrè, 1998, a pagina 269 si riferisce più specificamente all'eliminazione dei reati associativi di carattere generale e la loro sostituzione con <<fattispecie che perseguano un programma strumentale o finale ben circoscritto>>.
[379] Oltre a richiamare il pensiero di De Francesco visto precedentemente, si cita anche, nello stesso senso: De Vero, *Tutela penale dell'ordine pubblico. Itinerari ed esiti di una verifica dogmatica e politico-criminale*, Giuffrè, 1988, pag. 274.
[380] Riguardo a questo, si richiama alla trattazione eseguita nel punto 2 c).
[381] Spagnolo, *op. cit.,* pag. 1164.
[382] Patalano, *L'associazione per delinquere*, Jovene, 1971,pag. 94.
[383] Spagnolo, *op. cit.,* pag. 1164.

programma, dando vita ad una <<una sorta di probatio diabolica>>[384] sulle spalle di quest'ultima.

Onde evitare questo, l'Autore suggerisce che, qualora venisse accolta quest'ultima teoria, sarebbe allora preferibile <<riferirsi all'adeguatezza in negativo>>[385], ossia escludere la configurazione del reato tutte le volte che l'associazione si dimostri avere una struttura totalmente inadeguata per l'attuazione del programma delittuoso.

b) Riguardo invece la possibilità di sostituire il reato associativo descritto in <<termini generali>> con diverse fattispecie differenziate e aventi un ambito d'applicazione ben circoscritto, Spagnolo esprime tutto il suo rammarico[386] nell'ingiustizia che vi sarebbe nel prevedere lo stesso trattamento sanzionatorio per associazioni a delinquere aventi come obiettivo la realizzazione di delitti-scopo di lieve gravità rispetto a quelle che si prefiggono come scopo la commissione di reati ben più gravi.

Egli, riporta brevemente come esempio[387] un confronto tra un'associazione a delinquere che intende commettere come tipologia di reato la pubblicazione di foto oscene ed un'altra che invece commette sequestri di persona a scopo d'estorsione: mentre nel primo caso la pena prevista per il reato associativo è molto più grave di quella prevista per il delitto-scopo, nel secondo caso succede esattamente il contrario.

Sostenendo dunque il pensiero di alcuni autori enfatizzanti l'impossibilità di <<costruire per i reati associativi un oggetto di tutela del tutto indipendente dalle caratteristiche dei reati-scopo>>[388], si ritrova la netta predisposizione dell'Autore all'idea di disporre diverse fattispecie associative specifiche, volte a punire però solo quelle tipologie di associazioni che perseguano un programma particolarmente grave e con la previsione di un trattamento sanzionatorio diversificato per ogni singola fattispecie.

Quest'idea è realizzabile, per l'Autore, tramite due percorsi diversi:

---

[384] *Ibidem.*
[385] *Ibidem.*
[386] *Ivi,* pag. 1165.
[387] *Ibidem.*
[388] *Ivi,* pag. 1165, cita: De Vero, *op. cit.,* pag. 270.

1) Prevedere <<un reato base>> [389] ,volto a punire associazioni aventi un programma delittuoso con oggetto la commissione di delitti di media gravità, e tutta una serie di aggravanti per le associazioni che abbiano come scopo la commissione di delitti ben più gravi;

2) Predisporre diverse ed autonome fattispecie associative di carattere generale, distinte sulla base della tipologia di programma (strumentale e finale). Per questa seconda soluzione, il Legislatore dovrebbe dare la possibilità che le associazioni a delinquere abbiano come scopo la commissione di diversi delitti, nonché l'eventualità di prevedere- <<se riterrà giusto evitare il concorso formale di reati - una clausola di esclusione in favore del reato più grave>>.[390]

Se il Legislatore però scegliesse questa seconda opzione, sarebbe necessario che venissero fissati principi e criteri generali per l'associazione a delinquere, in modo da poter mantenere l'adeguatezza della misura penale contro la costante evoluzione del fenomeno dell'associazione a delinquere , ma anche al fine di eliminare tutte quelle incongruenze e difficoltà interpretative, <<frutto di una legislazione frammentaria e non coordinata>>.[391]

Come si è potuto notare, forse l'unico punto fermo nelle diverse riflessioni trattate rimane l'esclusione dell'opzione che vede la cancellazione della fattispecie di reato dal sistema: per il resto, sembrerebbe che ancora vi siano fin troppe e diverse prospettive sulle possibili riforme della norma incriminatrice.

Senza azzardare a formulare in questa sede una possibile ipotesi di riforma, occorre comunque notare che gli Autori sembrano focalizzarsi solo su un singolo aspetto della fattispecie, ergendolo ad unico criterio sulla cui base formulare le loro ipotesi d'innovazione[392].

In definitiva, bisognerebbe piuttosto considerare tutti gli elementi della fattispecie (e i problemi interpretativi legati ad ogni singolo elemento) per poter eventualmente formulare un'ipotesi di riforma: lavoro tutt'altro che semplice, ma che permetterebbe l'elaborazione di una fattispecie penale dai contorni ben definiti, in grado di punire le diverse tipologie di

[389] *Ivi*, pag. 1166.
[390] *Ivi*, pag. 1165.
[391] *Ivi*, pag 1166.
[392] Ad es., per Insolera è il bene giuridico come criterio di distinzione tra l'art. 416 e l'art. 110 c.p., per De Francesco è l'organizzazione; per Spagnolo la tipologia di programma.

associazione che si affacciano (e si affacceranno in futuro) nel panorama nazionale e transnazionale.

E - come si vedrà nella parte finale di questa trattazione - una riforma in questo senso dell'articolo 416 c.p. potrebbe esser di grande ausilio per la giurisprudenza, sempre più spesso oggi intenta ad uno sforzo interpretativo notevole al fine di ricondurre le nuove organizzazioni criminose nella fattispecie associativa.

Capitolo II - Il fenomeno del Cybercrime

In questi ultimi trent'anni, la crescita esponenziale di una tecnologia in grado di elaborare e diffondere informazioni <<con velocità e semplicità prima sconosciute>>[393] ha realizzato la creazione di un vero e proprio <<mondo>>, capace di estendersi ad ogni singolo aspetto della vita quotidiana; un luogo dove chiunque può inoltrarsi, finanche perdersi , e – a prescindere se essa abbia le competenze tecniche o meno - dove la persona può anche sentirsi libera da qualsiasi regola, poiché << all'interno di essa [della rete, N.d.A.] esiste la possibilità di espressione massima di ogni propria intimità comportamentale>>[394].

La definitiva apertura del vaso di Pandora è avvenuta poi con il fenomeno di massa di Internet, che ha permesso lo sviluppo di nuove forme di criminalità strettamente legate a queste nuove tecnologie, tutte riunite in una nuova enorme sfida per il giurista: il<<crimine cibernetico>>, meglio definito come *cybercrime*.

In questo capitolo, oltre ad eseguire una disamina generale sulla disciplina di questa realtà intrisa di diverse sfaccettature, si cercherà di porre in evidenza come la stessa metta in dubbio non poche categorie del diritto tradizionale (nazionale e sovranazionale), facendo emergere un nuovo compito per il giurista ed il Legislatore: occuparsi di questo << nuovo modo di essere del diritto >>[395], con tutti i problemi derivanti dalla sua applicazione e in considerazione della costante evoluzione dinamica del sistema cibernetico ed informatico.

1. Il passaggio dal computer crime al cybercrime

Spesso quando si pensa al concetto di cybercrime, la mente di chi non è giurista - o anche del giurista che non si è mai affacciato all'approccio di questa tematica - immediatamente

[393]Picotti, *Presentazione*, in Id. (a cura di),*Il diritto penale dell'informatica nell'epoca di Internet*, CEDAM, 2005, pag. VII.

[394]Maietta, *In tema di I.A.D., internet addictiondisorder,* in *Dir .Dell'Int*., n.2/2007, pag. 201. In conformità a questa visione: Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in Cadoppi, Canestrari, Manna, Papa(a cura di), *Cybercrime,* UTET Giuridica, 2019,pag. 40; Borruso, voce *Informatica giuridica,*in *Enciclopedia del Diritto*, Giuffrè, 1997, il quale a pag. 672, paragona il mondo dell'informatica alla figura del <<Grande Fratello>> di Orwell, proprio perché in questo luogo si consente << il più spinto esercizio della libertà individuale in tutti i campi […] e con essa la più strepitosa ed imprevista rivincita dell'individuo sulla massa>>.

[395] Frosini, *Il Costituzionalismo nella società tecnologica*, in *Dir. Inf*., Vol. 36, fasc. 3, 2020, pag. 465.

lo ricollega a tutte quelle tipologie di reato che vengono commesse online. In realtà, l'argomento è molto più ampio e complesso.

Prima però di passare ad una enucleazione dei tratti essenziali dei cybercrimes, è necessario eseguire un breve quadro storico-temporale dell'evoluzione legislativa italiana sull'argomento[396], partendo dal concetto di informatica giuridica.

Pur avendo una definizione di essa con radici attestate già dalla metà del secolo scorso[397], il vero e proprio sviluppo dell'informatica giuridica avviene in Italia circa nell'ultima fase del secolo scorso, e se ne può suddividere l'evoluzione in tre momenti:

1. La fase <<documentario-informativa>>[398]: corrisponde all'incirca agli anni '70, dove viene percepita l'informatica come strumento per organizzare meglio tutte le fonti legislative. Accanto allo sviluppo di banche dati legislative, si affianca la nascita di <<programmi redazionali>>[399], in grado di agevolare la produzione di atti e documenti.
   Oltre a sorgere i primi contrasti con le categorie tradizionali del diritto, questa fase viene definita come <<fase dei diritti dell'informatica>>[400]: non c'è ancora né una visione d'insieme né una dimensione definita, per cui per il momento non si può parlare di diritto dell'informatica come un *corpus* normativo unitario e ben delineato.

2. La fase <<meta documentario-decisionale>>[401]: corrisponde alla fase dei pieni anni'80 fino alla fine degli anni '90, ed è caratterizzata da due aspetti in particolare:

- L'iniziale sviluppo di ricerche scientifiche aventi ad oggetto l'intelligenza artificiale: nascono i primi progetti riguardanti <<programmi che, a partire da una conoscenza pre-

[396]Al fine della ricostruzione fatta nel testo, è stato molto utile un autore che accompagnerà tutta questa seconda parte della trattazione: si tratta di Picotti, con particolare riguardo al capitolo "*Diritto Penale e tecnologie informatiche: una visione di insieme,* in *Cybercrime,* (a cura di) Cadoppi et al., pagg. 35-69; Id., *Cybercrime e Diritto Penale,* in *Diritto Penale dell'Informatica*. *Reati della rete e sulla rete*, (a cura di) Parodi, Sellaroli,Giuffrè 2009, pagg. 709-723. Non bisogna poi trascurare l'importante contributo di Taddei Elmi e Peruginelli, *Dall'informatica giuridica al diritto dell'internet*, in *Diritto di Internet*, 2006, fasc.6 ,pagg.113-116.

[397]Si attesta che Loevinger in *Jurimetrics: The Next Step Forward*, in *Minnesota Law Review,* 1949, vol. 33, pag.455 e ss, definisca la c.d. <<giurimetria>>, ossia i tre ambiti dell'informatica giuridica. Secondo l'Autore, questi tre ambiti sarebbero: l'ambito informativo, l'ambito logico-decisionale e l'ambito statistico-previsionale. Per maggiori approfondimenti sul punto: Taddei Elmi, *L'informatica giuridica: disciplina o ricerca?,*in *Ciberspazio e diritto*, 2006, Vol.7, n.2 pagg. 244-245.
Si veda anche: Borruso, (voce) *Informatica giuridica,*in Enciclopedia del Diritto, 1997, Giuffrè, pag. 641.

[398]Taddei Elmi e Peruginelli, *op. cit.,* pag. 113.

[399]*Ivi,* pag. 114.

[400]*Ibidem.*

[401]*Ivi,* pag. 113.

organizzata, conducono attraverso un processo logico a soluzioni di problemi>>[402], in grado dunque di compiere processi decisionali[403].

- Non vi è ancora una concezione unitaria di informatica giuridica: piuttosto, c'è la presenza di una moltitudine di diverse tipologie di informatiche giuridiche (es. quella manageriale, quella decisionale, ecc.). Emerge però l'intenzionalità di dare una unitarietà alla disciplina dell'informatica giuridica, al fine di distinguerla dal diritto dell'informatica: se il secondo è <<una disciplina giuridica dove il diritto è lo strumento e la tecnologia l'oggetto>>[404], l'informatica giuridica è invece <<un ambito dell'informatica dove la tecnologia è lo strumento e il diritto è l'oggetto>>[405].

Questa fase raggiunge il suo culmine con l'entrata in vigore della legge numero 547 del 23 dicembre 1993 (<<Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica>>), inserita nel libro II del Codice Penale.

Facendo una breve parentesi su di essa,si comprende che questa legge è stata adottata dal Legislatore italiano in seguito all'esigenza di predisporre delle previsioni specifiche riguardo comportamenti particolari: ossia, <<condotte poste in essere contro (o per mezzo dell'uso di) sistemi informatici>>[406]. In particolare, si è deciso di prevedere la punibilità di alcune tra queste condotte senza tuttavia inserire nel codice penale una sezione *ad hoc* dedicata ai reati informatici, ma introducendo alcune fattispecie nella parte speciale del codice penale[407] – e, in via secondaria, disponendo una legislazione complementare al codice (es. la legge numero 445/2000, che ha introdotto nuove forme di tutela per il diritto d'autore via Internet[408]).

---

[402] *Ibidem.*

[403] *Ibidem.*Si collocano due limiti di base a queste intelligenze artificiali: uno è un limite quantitativo (<<la difficoltà di rappresentare in modo formalizzato ampi settori del diritto>>); il secondo è invece un limite qualitativo, ossia l'impossibilità di arrivare a produrre una norma seguendo solo metodi esclusivamente logici e matematici. Per maggiori approfondimenti sul tema, si veda: Picotti, *Diritto Penale e tecnologie informatiche: una visione di insieme*, in Cadoppi et al., *Cybercrime*, pag. 45.

[404] *Ibidem.*

[405] *Ibidem.*

[406] Alma e Perroni, *Riflessioni sull'attuazione di norme a tutela dei sistemi informatici*, in Diritto Pen. e Proc., n. 4/1997, pag.504.

[407] Per maggiori approfondimenti, si fa riferimento a: Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Id.,*Il diritto penale dell'informatica all'epoca di Internet*, CEDAM, 2005, pagg. 44 e ss.. In particolare, si fa riferimento ai vantaggi che si ottengono da questa scelta del Legislatore: in primis, si mantiene la classificazione delle diverse tipologie di reato del Codice Penale Italiano; ma anche si ha la possibilità di evidenziare <<i parallelismi e le analogie con quelle [le norme] preesistenti>>, pag. 46.

[408] Per maggiori approfondimenti sul punto: Pascuzzi, *La tutela del diritto d'autore nell'epoca digitale*, pagg.301-309; Seminara, *La tutela penale del diritto d'autore tra norma vigente e prospettive di riforma*, pagg.311-340, entrambi in.: Picotti, *Il diritto penale dell'informatica nell'epoca di Internet*, cit. .

Tuttavia, l'introduzione delle nuove fattispecie criminose ad opera della legge 547/1993 portava con sé non pochi dubbi interpretativi[409]. Queste incertezze, in realtà, sono dovute ad una caratteristica di fondo: i reati introdotti con la legge 547 del 1993 sono considerati <<realizzabili in singoli sistemi *stand alone*, connessi solo eventualmente in reti telematiche chiuse o ad accesso circoscritto>>[410].

C'è dunque un tema di fondo finora non ben esplicitato: il sistema informatico del tempo non ha le caratteristiche di quello odierno, ma è piuttosto un sistema ancora prevalentemente composto da banche dati e rivolto a settori economici, ma soprattutto è ancora un sistema chiuso, in cui solo pochi soggetti previamente autorizzati possono accedere, proprio perché esso è rivolto in particolare all'utilizzo da parte di ricercatori e studiosi nell'ambito tecnologico ed informatico, con regole proprie che il gruppo ristretto usufruente del sistema rispettava scrupolosamente[411].

Si aggiunge che c'è anche chi sostiene[412] che vi sia anche da addossare una responsabilità al giurista in tutto questo: egli, piuttosto che cooperare col legislatore in questa tematica- nota per i suoi cambiamenti rapidi e costanti- scegliendo di sforzarsi nell'attività interpretativa rispetto alle diverse fattispecie concrete, si è dimostrato piuttosto indolente, invocando solo l'intervento del legislatore sulla materia. Questo ha contribuito a far sì che la legislazione penale in materia sia divenuta<<quasi subito già superata o inadeguata>>[413].

3. Tutto cambia nella fase <<reiziaria>>[414], corrispondente all'apertura di Internet[415] al pubblico globale: grazie ai c.d.<<protocolli di comunicazione tra reti e sistemi diversi>>[416]

---

[409]Per fare qualche esempio, nello stesso articolo summenzionato di Alma e Perroni si enuncia come uno dei reati introdotti grazie alla legge 547 sia l'accesso abusivo ai sistemi informatici o telematici (art. 615- ter c.p.): considerando che nello stesso articolo viene prevista l'aggravante nel caso in cui il fatto è commesso <<con abuso delle qualità di operatore del sistema>>; il legislatore non aveva specificato con chiarezza quando poteva esserci un <<accesso abusivo>> al sistema: questo creava delle difficoltà nell'individuare la presenza dell'abusività dell'accesso in non pochi casi (ad es., il caso spiegato nelle pagine 504-506, fa riferimento all'ipotesi in cui l'agente fosse un operatore informatico -in grado dunque di poter accedere, nell'ambito del proprio lavoro,a tutte le informazioni presenti nel sistema informatico- che occasionalmente entrava non col proprio codice di accesso, ma con quello dei suoi colleghi di lavoro).

[410]Picotti, *Diritto Penale e tecnologie informatiche, cit.*,pag. 47.

[411] De Rosa, *La formazione di regole giuridiche per il "Cyberspazio*", in *Dir .inf.,* 2003, fasc. 2, pag.361, parla appunto di <<netiquette>>, ossia un'insieme di regole utilizzate dagli utenti disciplinanti sia l'aspetto meramente tecnico delle informazioni comunicate, ma anche un'insieme di regole etiche che ciascun utente deve seguire. V. anche in seguito.

[412]Borruso, (voce) *Informatica giuridica,* in*Enc. Dir.*, Giuffrè,1997, pag.672.

[413]*Ibidem.*

[414]Taddei Elmi e Peruginelli*, op. cit*., pag. 113.

[415]Importante però precisare come, ricordato da De Rosa,*op .cit*.,pag. 362, seppur venga definita spesso Internet come la <<regina delle Reti>>, essa non è l'unica Rete informatica presente: questo perché esistono anche altre reti informatiche o telematiche che hanno una portata più ristretta rispetto al numero di utenti e/o

(creanti il famoso www)si realizza il passaggio da una Rete informatica<<chiusa>> e accessibile per pochi ad un vero e proprio fenomeno di massa, definito addirittura come <<un luogo anarchico del sito libero>>[417]: la rapidità e la quantità di informazioni scambiate grazie alla rete informatica unita alla globalità e fruibilità per chiunque[418], creano un vero e proprio sconvolgimento d'ogni singolo aspetto dei rapporti sociali,politici, economici e culturali, ponendo in essere quella che si definisce come <<società postindustriale […]>> o, meglio ancora, <<società informatica>>[419], ancora oggi in fase di sviluppo.

Questa è una fase che forse definire rivoluzionaria è riduttivo, considerato che con essa avvengono diversi cambi di rotta. *In primis*, vi è un cambio di prospettiva in relazione al diritto dell'informatica: non c'è più la considerazione del diritto dell'informatica come una serie di disposizioni <<appartenenti a settori giuridici diversi>>, quanto piuttosto la prepotente esigenza di qualificazione della categoria di diritto dell'informatica come un<<diritto autonomo […],basato su una teoria specifica>>[420], nonché sorgono nuovi diritti e beni giuridici da tutelare (come numerosa dottrina permette di cogliere)[421]. Da ultimo, questa <<fase reiziaria>> segna il decisivo passaggio dalla mera informatica ad una dimensione molto più ampia: si tratta del Cyberspace (o Cyberspazio)- di cui non si ha propriamente una nozione univoca – poiché è quello spazio[422] che è sia spazio delle interazioni delle intelligenze artificiali create dall'informatica, ma è allo stesso tempo uno

---

ai computer collegati ad essa- si sta parlando appunto delle reti L.A.N. (<<Local Area Network>>), che possono essere chiuse o aperte a seconda se esse consentano o meno lo scambio di dati con altre reti.

[416]Picotti, *Diritto Penale e tecnologie informatiche*,in Cadoppi et al., *Cybercrime*, cit., pag. 46.

[417]Alma e Perroni, *op. cit*. , pag. 114

[418]Sull'impatto di Internet sulla conoscenza in generale, si veda, per maggiori approfondimenti: Pascuzzi, *Il diritto dell'era digitale*, pagg. 25-27.

[419] Borruso, *op. cit*., pag. 674. Si veda anche: Picotti, *Sistematica dei reati informatici,tecniche di formulazione legislativa e beni giuridici tutelati*, in Picotti, *Il diritto penale dell'informatica nell'epoca di Internet*, 2005, CEDAM, pag. 29.

[420]Taddei Elmi e Peruginelli, *op. cit.,* pag. 114.

[421]Per maggiori approfondimenti sul punto, si cita come esempi: Eusebi, *Anonimato, identità personale e diritto di cronaca nel mondo telematico. La sentenza della Corte di Cassazione n. 5525/2012*, in *Ciberspazio e diritto*, vol. 14 n.48 (2-2013), pagg. 183-209; Lavacca, Artini, Pellegrino, *Internet "never forgets"(?). Diritto all'oblio e diritto alla cancellazione, quali gli usi e quali i limiti*, in *Ciberspazio e Diritto*, vol. 20, n. 63 (3-2019), pagg. 437-461; Frosini, *Il Costituzionalismo nella società tecnologica*, in Dir. Inf., Vol. 36, fasc. 3, 2020, pag. 465 e ss.; Mucciarelli, *Informatica e tutela penale della riservatezza*, in Picotti, *Il diritto penale dell'informatica nell'epoca di Internet*, CEDAM, 2005, pagg. 173-183.

[422]Picotti, in *Cybercrime e diritto penale,* a pag. 710 sottolinea come la definizione deriverebbe da kyber , (<<timoniere>> o <<pilota>>in greco), utilizzata per la prima volta da Wiener in *Cybernetics: Or Control and Communication in the Animal and the Machine*, cit.,1948; allo scopo di definire una nuova scienza che studi il modo in cui <<uomini, animali e macchine comunichino con l'ambiente esterno e lo controllino>>.

spazio dove ciascuno di noi è immerso e allo stesso tempo connesso costantemente con gli altri[423].

Più specificamente, il Cyberspazio può esser immaginato come composto da tre <<livelli>> distinti, ma, allo stesso tempo,sovrapposti l'uno all'altro ed in costante relazione fra loro. Alla base c'è lo strato tecnologico, il <<motore>>che permette il funzionamento del Cyberspazio: esso è in costante mutamento, in quanto<<risponde alle necessità del mercato, dei governi, delle multinazionali e degli attori che fruiscono dei servizi proposti>>[424].
Poi c'è il livello mediano, definito come <<strato sociale>>[425]: corrisponde allo spazio dei consumatori. In esso vengono svolte la stragrande maggioranza delle attività nel Cyberspazio (dal gioco alla comunicazione, all'ambito produttivo, ecc.), nonché tutte le interazioni della quotidianità. L'ultimo livello al vertice è <<lo strato di *governance*>>[426]., dove si svolgono due importanti funzioni: la prima è l'incontro tra le società hi-tech (in particolare, le multinazionali del settore IT, le c.d. <<Big Five>>[427]) e le pubbliche istituzioni al fine di definire i limiti e le regole del cyberspazio; la seconda è la realizzazione dell'offerta rivolta ai consumatori del cyberspazio, nonché la formulazione di nuove idee per creare nuova domanda per i consumatori.

Bisogna, infine, considerare due aspetti fondamentali che caratterizzano il Cyberspazio. Il primo è la <<iperconnettività>>[428], perché la velocità con cui i dati vengono acquisiti, elaborati e trasmessi è possibile grazie alla costante condivisione di numerosi utenti di diverse parti del mondo, permettendo anche il raggruppamento di questi dati in insiemi enormi e complessi (i c.d. <<Big Data>>[429]);

---

[423]La definizione è tratta da: De Rosa, *op. cit.,* pag.361. Cfr. anche Picotti *in Cybercrime e diritto penale,* pag. 710, secondo cui il Cyberspazio non è solo mero spazio <<virtuale>>, poiché è ormai <<una dimensione imprescindibile della nuova realtà sociale, con un ruolo propulsore della complessa realtà in cui viviamo>>[423].
[424]Tonellotto, *Criminalità e cyberspazio, alcune riflessioni in materia di cyber criminalità,* in *Rivista di Criminologia, Vittimologia e Sicurezza*, 2022, Vol. XVI, pag.7.
[425]*Ibidem.*
[426]*Ibidem.*
[427]Conosciute in Italia come <<GAFAM>>, si tratta delle cinque multinazionali dell'IT (Google, Apple, Facebook, Amazon e Microsoft), conosciute anche per il loro gigantismo e per esser divenute una scelta <<obbligata>> per l'utente. Per maggiori informazioni sulle loro caratteristiche, si fa riferimento a quanto riportato da Wikipedia (https://it.wikipedia.org/wiki/GAFAM).
[428]Picotti, *Cybercrime e diritto penale,* cit., pag. 710.
[429]Della Morte*, Big data e protezione internazionale dei diritti umani*. *Regole e conflitti*, Editoriale scientifica,2018,. Per maggiori approfondimenti, si cita: Pascuzzi, *Il diritto dell'era digitale*, , Il Mulino, 2020,pagg.265-279.

Il secondo è l'<<automazione>>[430]: partendo originariamente dalla mera elaborazione sul calcolo matematico effettuata dai primi computer[431] , grazie all'invenzione di numerosi programmi oggi è possibile <<l'applicazione […] di algoritmi sempre più complessi, in grado [anche] di auto-apprendere e correggersi>>[432].

Queste ultime due precisazioni permettono di affrontare la trattazione dell'ultima - ma non meno importante - novità: se lo <<spazio>> di interazione si espande a livello globale ed oltre la dimensione informatica, è chiaro che nel Cyberspazio emergono anche nuovi comportamenti illeciti, meritevoli di essere puniti.

Seppur per lungo tempo è stata presente nel web una <<autoregolazione>>[433] con l'utilizzo dei soli codici tecnici (sulla base del principio <<Code is Law>>[434]), oggi non si può considerare il cyberspazio come un luogo esente dall'applicazione del diritto: tenendo in considerazione il principio secondo cui<<ciò che è illecito offline non può esser lecito online>>, è necessario che ci si occupi in primo luogo di costruire un <<quadro giuridico generale>>[435], in modo da rilevare quali possono essere i comportamenti illeciti online in questa nuova realtà - diversa da quella di cui il diritto tradizionale si è sempre occupato finora.

1.1.La distinzione tra reati cibernetici e reati informatici

Secondo una comunicazione della Commissione Europea, il cybercrime è composto da tutti quei reati <<commessi contro le reti di comunicazioni elettroniche ed sistemi di informazione o avvalendosi di tali reti e sistemi>>[436].

Da questa definizione si ricava in primo luogo una prima fondamentale distinzione: vi sono reati che utilizzano la tecnologia ed il sistema tecnologico come strumento per la

[430]Picotti, *Cybercrime e diritto penale,* pag. 710.
[431]Per un maggior approfondimento sull'evoluzione del computer e sulla nozione di esso da un punto di vista giuridico, si rimanda a: Borruso, *op. cit*., pagg.642-647.
[432]Picotti, *Cybercrime e diritto penale,* pag. 710.
[433]Per maggiori approfondimenti sul tema,e sulla nozione di <<sovranità digitale>>, si cita: Pascuzzi, *op. cit*, pagg. 347-352.
[434] Lessig, *Code and OtherLaws of Chyberspace*, 2006, Basic Books.
[435]*Ivi*,pag. 42.
[436]Si fa riferimento a:*Communication from the European Commission to the European Parliament, The Council and the Committee of the regions: Towards a general policy on the fight against cybercrime*, COM(2007) 267.

commissione del reato stesso, altri casi in cui invece è lo stesso sistema cibernetico o informatico ad esser l'oggetto materiale verso cui si dirige la condotta illecita[437]; nonché ipotesi in cui la condotta criminosa mediante le TIC sia ricavabile in via interpretativa dalle fattispecie penali equivalenti ovvero casi in cui essa sia già espressamente prevista nella norma.

Da queste semplici distinzioni, il reato sarà neisecondi casi<<in senso stretto>>, nei primi invece <<in senso lato>>.

Altra distinzione fondamentale da compiere è quella tra reati cibernetici ed informatici: nel primo caso, la fattispecie sarà incentrata sugli strumenti o gli oggetti informatici; nel secondo caso la fattispecie viene definita dalla dottrina come <<categoria aperta>>, perché comprendente non solo i mezzi e gli oggetti informatici, ma anche tutti gli altri comportamenti posti << avvalendosi (anche) di Internet e alla tecnologia delle telecomunicazioni>>[438].

Da queste due distinzioni si possono ottenere dunque quattro diverse categorie[439].

1. I reati <<informatici in senso stretto>>[440]: ad essi corrispondono tutti quei reati nella cui fattispecie si richiamano espressamente le TIC (<<tecnologie dell'informazione e della comunicazione>>): che sia, alternativamente, nella descrizione della condotta, nell'evento, o in altre condizioni del reato, è essenziale che sia presente l'elemento informatico affinché la fattispecie di reato sia integrata (es.: il sistema <<informatico o telematico>>, dati, informazioni o programma <<informatico>>, documenti <<informatici>>, ecc.). Un esempio di questa tipologia di reati è l'accesso abusivo ad un sistema informatico o telematico[441], art. 615 *ter* c.p.

[437]È comunque importante precisare che, seppure il sistema informatico o cibernetico sia il <<bersaglio>> di queste condotte illecite, il bene giuridico leso o messo in pericolo in realtà sarà altro: ad es., se il sistema informatico è il target dell'attività terroristica il bene giuridico minacciato sarà però la personalità dello Stato; se tramite un virus o un malware vengono acquisite e poi rese pubbliche informazioni o foto private, il sistema informatico ha subito l'attacco, ma il bene giuridico leso è senza dubbio la persona, ecc. .

[438]Picotti, *Sistematica dei reati informatici,* pag.58.

[439]Picotti le elenca in *DirittoPenale e tecnologie informatiche: una visione di insieme*, nelle pagg. 76-88.

[440]*Ivi*,pag. 75.

[441]Come indicato da *Ivi*, pag. 65, l'accesso abusivo è posto allo scopo di incriminare <<ogni oggettiva violazione dell'esclusiva disponibilità , in capo al titolare, degli spazi informatici di cui ha diritto […], in quanto instaura un *rapporto conflittuale* […] riguardo non solo le procedure informatiche che *tecnicamente* abilitano e legittimano l' "introduzione" e l'utilizzo del sistema, ma anche riguardo alle regole e disposizioni generali […] poste dal titolare del sistema […] per regolare il successivo "mantenimento" in tali spazi […]>>.

2. A differenza di quelli in senso stretto, <<i reati informatici in senso ampio>>[442], sono invece quei reati che si <<possono realizzare anche mediante strumenti o oggetti informatici, […] compreso il web>>[443]. In questo caso, l'elemento informatico è presente nella fattispecie come possibile modalità, oggetto o strumento della condotta; ovvero non è indicato espressamente nella norma, ma è ricavabile in via interpretativa se la fattispecie penale è compatibile con le TIC.
   Un classico esempio è di questa categoria sono quelle tipologie di reati riguardanti la diffusione di contenuto illecito online, ma che può avvenire con altri mezzi di comunicazione: ad es. la pedopornografia virtuale, ex art. 600-*quater* c.p.

3. Come detto precedentemente, i reati cibernetici <<sono tutti quelli che si possono commettere […] nel Ciberspazio>>[444]; ma per i reati <<cibernetici in senso stretto>>[445] si richiede che sia necessariamente indicata la rete come elemento essenziale della fattispecie o come circostanza. Un esempio di reato cibernetico in senso stretto è il c.d. cyberstalking, ossia l'art.612-bis[2] c.p., un'aggravante del reato di atti persecutori [446] che richiama espressamente le TIC;

4. Nei reati cibernetici in senso ampio, la rete è una eventuale o compatibile modalità della condotta, elemento costitutivo del fatto tipico o evento. Al pari dei reati informatici in senso ampio, il riferimento alla dimensione cibernetica non è necessario che sia specificato, ma può esser ricondotta la fattispecie a questa categoria in via interpretativa se essa è compatibile con le TIC.

   Come afferma Picotti,<<tutti i "reati cibernetici in senso stretto" sono logicamente anche "reati informatici in senso stretto"[…], ma non è vero l'inverso>>[447]: considerato che nel Ciberspazio sono compresi i sistemi informatici, è chiaro che nella fattispecie deve imprescindibilmente esser presente un esplicito richiamo al Ciberspazio (ossia, un espresso riferimento alle TIC nella disposizione). Tuttavia, la presenza dell'elemento informatico

[442] *Ivi*, pag. 76.
[443] *Ibidem.*
[444] *Ivi,*pag. 77.
[445] *Ivi*, pag. 78.
[446] Riprendendo l'art. 612-bis[2] c.p., <<la pena è aumentata […], se il fatto è commesso attraverso strumenti informatici e telematici>>. Considerando che lo stato di paura o di ansia della vittima si realizza tramite la ripetizione di comunicazioni, la modalità di condotta con la specifica indicazione delle TIC - secondo Picotti, *op. cit.,* pag. 78 – comporta che la condotta stessa non possa che realizzarsi nel Cyberspazio (che può essere su Internet, ovvero altre reti di telefonia o messaggistica).
[447] *Ibidem.*

della fattispecie non implica necessariamente che il reato si consumi esclusivamente su Internet, ma può anche <<concepirsi in un sistema chiuso>>[448].

Di conseguenza, quelli che sono reati informatici in <<senso stretto>> secondo questa impostazione sono necessariamente anche <<reati cibernetici in senso ampio>>.

In realtà, queste classificazioni non sono così rigide[449] ed i loro confini sono molto più labili di quello che sembrano: considerato che il Cyberspazio riguarderebbe tutte le tipologie di reato che si realizzano in esso, si deve affermare che la categoria dei reati cibernetici in effetti si sta sempre più estendendo col tempo, proprio per l'emersione di sempre più condotte offendenti diverse tipologie di beni giuridici[450] <<che diventano sempre più temibili, richiedendo adeguate risposte a livello normativo, oltre che investigativo>>[451].

Oltre a quanto detto finora, bisogna aggiungere ulteriori considerazioni riprendendo brevemente l'impatto di Internet[452]. L'accesso globale alla Rete, grazie sia alla presenza di <<software amichevoli, i quali consentono di navigare e scambiare informazioni anche ai non esperti>>[453], sia al potenziamento degli <<hardware>>[454], ha creato una <<duplice rivoluzione>>[455]. Analizzando un primo aspetto di essa, con l'apertura di internet al pubblico globale, non solo si è passati da un sistema <<chiuso>> ad uno <<aperto>>(come

[448] *Ibidem.*

[449] Ciò sarà reso più evidente sia da una seconda tipologia di classificazione di reati cibernetici, presente nella generale trattazione del profilo criminologico dedicato alle vittime ed autori di queste tipologie di reati (par. 2.1.3.); la terza sarà quella indicata nella Convenzione di Budapest, di cui si tratterà in seguito nel par. 2.2.

[450] Un chiaro esempio in questo senso ci è fornito da Picotti, *Cybercrime e diritto penale*, pagg. 714-5: ossia, l'aumento della previsione di aggravanti di condotte <<che si possono manifestare anche off line>>. Es. il cyberstalking,il *cyberbullism*o o il *revenge porn*.

[451] Picotti, *Cybercrime e diritto penale*, pag. 715.

[452] La definizione d'Internet si ritrova in: Pica, *(voce) Internet*, in *Digesto delle discipline penalistiche,* 2004, UTET, pag. 429.<<Internet non è luogo né spazio, ma è soltanto <<software>>: è una metodologia di comunicazione ipertestuale che consente l'accesso- e quindi lo scambio- di qualsiasi contenuto digitale posto su sistemi informatici connessi alla Rete attraverso tale modalità ipertestuale>>.

[453] *Ivi,* pagg.429-430, si fa in particolare riferimento al protocollo base di Internet, il c.d. TCP/IP (<<Transmission Control Protocol/Internet Protocol>>), un insieme di diversi protocolli di applicazione che ha permesso a sistemi diversi di poter comunicare tra loro, anche se aventi una diversità strutturale. Inoltre, bisogna ricordare il <<principio di neutralità della rete>>, che si ritrova nella direttiva UE 2018/1972, sulla base del principio della «neutralità tecnologica» (art. 4, lett. c), volto a garantire la non imposizione dell'uso di una particolare tecnologia rispetto alle altre, il principio di neutralità della rete è volto ad impedire la discriminazione nell'accesso ad Internet, nonché l'impegno a fornire le garanzie e i mezzi adeguati per mantenere Internet una rete <<aperta>>.
Per maggiori approfondimenti, si cita: Pascuzzi, *Il diritto dell'era digitale*, 2020, Il Mulino, pagg. 60-66.

[454] La definizione di hardware si ritrova anch'essa in: Pica, *op.cit*., pag. 430, corrispondente all'insieme di tutti quegli strumenti (es. cavi, router, server, ecc.) sulle quali <<transita la comunicazione>>. Come viene però correttamente ricordato nella stessa pag., l'hardware non rappresenta <<l'essenza di Internet>>, in quanto fa transitare qualsiasi forma di comunicazione telematica: l'hardware perciò può lavorare tranquillamente senza Internet.

[455] V. De Rosa, *op. cit.,* pag.361

visto precedentemente), ma è anche cambiata la tipologia di comunicazione: prima, considerato il cerchio ristretto e privato del sistema informatico, vi era una sorta di <<netiquette>>[456], una serie di principi di correttezza che venivano aspramente sanzionati se violati. Adesso invece, con l'apertura della Rete a tutti- chi cerca di ottenere profitti compreso- è stata sconvolta << la logica delle comunicazioni e delle informazioni diffuse in essa>>[457]- ecco perché questa prima rivoluzione viene definita come interna alla Rete.

La seconda è invece una rivoluzione sociale: oltre all'estensione del mondo virtuale ad ogni aspetto della vita quotidiana, bisogna menzionare anche come Internet tramite il <<bit>>[458]abbia non solo superato qualsiasi altra forma di comunicazione in quanto ad efficienza e velocità, ma anche abbia scardinato <<tutte le barriere, spaziotemporali, politiche, economiche, tecniche e giuridiche della comunicazione tradizionale>> [459], ponendo di conseguenza in crisi i meccanismi di essa.

Da quanto detto finora, si intuisce dunque come le problematiche emergenti nel rapportarsi a questo nuovo <<mondo>>siano sicuramente non esigue: a partire dalla distinzione non sempre agevole delle diverse tipologie di reati cibernetici ed informatici, nonché da una - ancor più pericolosa - infinita probabilità di creazione di future forme di reato e di altrettante diverse modalità di manifestazione delle condotte illecite (comprese anche delle fattispecie penali preesistenti nell'ordinamento).

Nella scelta se prevedere nuove fattispecie o introdurre nuovi commi a quelle preesistenti per la disciplina dei reati cibernetici (dubbio ancora preesistente)[460], occorre che il legislatore non trascuri una peculiarità del crimine cibernetico rispetto a quella del reato <<tradizionale>>: considerate le dimensioni in costante sviluppo del Ciberspazio, le tipologie di condotte illecite che si possono realizzare in esso non sono limitate, anzi:non solo il numero di tipologie di reato che si possono commettere è potenzialmente illimitato, ma anche il numero di vittime può divenire una cifra di valore incalcolabile. La ragione di ciò sta ne <<la crescente molteplicità di illeciti, di modalità di offesa dei beni giuridici, e di

---

[456]Pica, *op. cit.,* pag.436.Dalle parole <<net>> (rete) ed <<etiquette>>, se ne trae che la netiquette – prima che Internet diventasse un fenomeno globale- riprendeva i concetti di lealtà, correttezza e buona fede. Più specificamente, essa corrispondeva alla frase <<ricorda l'umano>>: ossia, ricordare che le informazioni trasmesse e/o ricevute nella rete sono sempre trasmesse da esseri umani, nonché di comportarsi nella rete allo stesso modo in cui ci si comporterebbe nella vita reale. Per ulteriori approfondimenti, si veda: De Rosa*, op .cit.,* pag. 361.

[457]*Ibidem.*

[458]La definizione di Bit (<<binarydigit>>, ossia cifra binaria) si ritrova in : Pascuzzi, *op. cit*.:, pag.37. Essa corrisponde ad <<un'unità di informazione che può essere rappresentata da zero o uno>> e può esser utilizzata per la formazione di un sistema binario.

[459]Pica,*op. cit,,*pagg.436-437.

[460]Picotti, *Sistematica dei reati informatici*, pag. 59

diritti anche fondamentali , che a loro volta si configurano come nuovi,quando siano essi stessi frutto del predetto sviluppo tecnologico>>[461].

1.2. Le tecniche abusive di acquisizione delle informazioni in rete a scopo di tracciamento.

Spesso, per la commissione di numerosi reati informatici (in senso lato) e cibernetici, gli autori di questi reati tendono ad utilizzare particolari software[462] o strumenti (leciti e illeciti) al fine di acquisire ovvero di controllare informazioni personali, in modo da poter effettuare un <<tracciamento dei profili degli utenti di Internet>>[463], intaccando la c.d.<<identità digitale>>[464]. Conseguentemente, è giusto soffermarsi brevemente sulle tipologie più note.

Lo <<spyware>> parrebbe esser lo strumento di spionaggio più comune: esso corrisponde a un programma, o incluso in programmi <<freeware>> (cioè programmi gratuiti, ma che in realtà non lo sono, <<perché hanno un prezzo, consistente appunto in una limitazione della privacy dell'utente>>[465]), ovvero scaricati dall'utente inconsapevole.
Di spywares ve ne sono di diverso tipo: vi sono quelli che si limitano ad acquisire informazioni utili al mondo imprenditoriale (che, si aggiunge, se vi fosse il consenso dell'utente, risulterebbero leciti). Ma sono una minoranza piuttosto esigua: la stragrande maggioranza tende ad acquisire un numero d'informazioni (purtroppo) molto invasivo

[461]Id., *Cybercrime e diritto penale*, pag. 715.
[462]La nozione di Software, ossia: <<programma o parte di programma, procedura, regola e documentazione associata di un sistema di elaborazione delle informazioni>>, necessario per il funzionamento di un sistema informatico, si riprende da: Pascuzzi, *op. cit*., pag. 36.Attualmente, a livello europeo, la disciplina del software è posta nella direttiva 2009/24/CE del Parlamento europeo e del Consiglio , in Gazzetta Ufficiale dell'UE del 5/05/2009.
[463] Pica,*op .cit.,* pag.434.
[464]L'espressione <<identità digitale>>, in base a quanto indicato da Pascuzzi, *op. cit*., pagg. 44-45, avrebbe 2 significati diversi:
- Un meccanismo pubblico (noto anche come SPID, <<Sistema pubblico di identità digitale>>) che garantisce a tutti i cittadini e alle imprese un accesso unico, sicuro e protetto ai servizi digitali della pubblica amministrazione e dei soggetti privati aderenti>>,
- <<la riferibilità a un soggetto di tutta l'attività compiuta>> nei sistemi informatici, telematici e cibernetici. In questa trattazione, si considererà la seconda accezione del termine. Interessante notare che, a differenza del primo caso, nella seconda ipotesi non c'è un organo che verifichi <<la corrispondenza di un'attività svolta nel mondo digitale a un certo soggetto>>: questo farebbe dunque emergere un interesse giuridico alla preservazione e al mantenimento della propria identità virtuale.

[465] Pica, *op. cit.*, UTET, pag. 431.

della sfera privata dell'utente[466], riuscendo addirittura anche ad aumentare enormemente la quantità di informazioni carpite in brevissimo tempo tramite il download d'altri programmi di auto-aggiornamento. E tutto questo- è necessario rimarcarlo apertamente- all'insaputa del soggetto cui le informazioni si riferiscono.

Alcuni autori considerano che in realtà la legge 547/1993 non avesse previsto la disciplina penale a tutela di queste situazioni. Oltre al fatto che -come si ricorderà - il fenomeno globale d'Internet avvenne successivamente l'entrata in vigore di questa legge, bisogna anche ricordare che è molto difficile ricomprendere queste ipotesi nelle fattispecie introdotte: si potrebbe eventualmente pensare all'art. 615-ter c.p., ma le acquisizioni delle informazioni avvengono tramite l'installazione di un programma da parte dell'utente, non con un accesso abusivo. Perciò, a meno che non siano chiaramente specificate le funzioni dello spyware, <<l'esistenza di intromissioni di dati non possono esser provate>>[467].

Un appunto finale da svolgere è il fatto che il trojan e lo spyware fanno parte del <<banking malware>>[468], uno dei meccanismi odiernamente maggiormente utilizzati per effettuare frodi bancarie nel cyberspazio.

Altro strumento da non ignorare è il <<Web-bug>>: esso è presente in un'immagine o logo di una pagina Web o in un messaggio di posta elettronica, e tramite esso si permette il monitoraggio di chi visita quella pagina o legge il messaggio, e si inviano le informazioni ottenute (es.:nome utente del soggetto,la password d'accesso della Rete al sito, data e ora in cui viene aperta la pagina o l'e-mail) al creatore del Web Bug o ad altri soggetti a cui sono utili le informazioni ottenute. Ma non solo- il Web Bug è uno degli strumenti chiave per la ricostruzione del profilo delle potenziali vittime:si è notato che spesso, incrociando le informazioni raccolte dal Web-bug e quelle raccolte da altre tecniche di tracciamento, risulta esser abbastanza semplice <<ricostruire un profilo dell'utente <<spiato>>>>[469].

A differenza dello Spyware, è abbastanza agevole rintracciare la presenza dei Web Bug: a questo scopo, è sufficiente appunto un'analisi della pagina Web (o della mail, a seconda

[466]*Ibidem*,ponecome esempi: il nome dell'utente, l'indirizzo IP, quali banner ha cliccato l'utente, quali files (che siano immagini, documenti, ecc.) siano stati scaricati, ecc.
[467]Pica, *op .cit.,* pag. 433.
[468]Bonavita, Cortina, Stringhi, *"Conosci il tuo nemico": un primo approccio tassonomico ai principali attacchi informatici nel settore del cybercrime bancario e finanziario*, in Ciberspazio e Diritto, vol.21, n.66, (3-2020), pag. 476.
[469]Ivi, pag. 435.

dei casi)con il linguaggio <<HTML>>[470]: i Web Bug si riveleranno essere degli <<HTML image tag>>, con all'interno un sito web diverso da quello della pagina analizzata e – guarda caso- corrisponde al sito a cui vengono inviate tutte le informazioni raccolte.

Nonostante vi sia odiernamente la presenza di numerosi software elettronici di protezione e un maggior studio su questo fenomeno[471], si deve notare come non tutti quelli che usufruiscono del Web hanno le conoscenze informatiche necessarie per compiere un'attività del genere e, anche se fosse, non sarebbe comunque in alcun modo possibile per loro né <<modificare la pagina Web che li contiene>>[472], ma nemmeno sapere quali informazioni sono state acquisite e recuperarle.

Notissimi sono poi i c.d. <<cookies>>[473], files d'informazioni che vengono costantemente registrati ed inviati dal computer dell'utente ad ogni accesso in ogni pagina , allo scopo di rendere più agevole e rapido un futuro accesso delle medesime pagine. Queste informazioni di solito riguardano quale frequenza il navigatore accede al sito, quante volte l'utente accede per personalizzare il sito o se effettua eventuali acquisti nel sito stesso.

Questi files sono leciti, perché posti a scopi pubblicitari/imprenditoriali e non vengono riferite le informazioni dell'utente contenuti in essi a soggetti specifici, in conformità all'attuale disciplina di tutela dei dati personali[474].

Tuttavia, <<sia nei casi in cui l'accesso a Internet sia fornito dallo stesso fornitore della connessione telefonica […]>>[475]sia nei casi di <<convergenza tecnologica>>[476], i dati acquisiti dai cookies possono esser trasmessi ad una persona fisica, senza alcun consenso dell'utente.

---

[470]Come indicato dalla pagina web Wikipedia (https://it.wikipedia.org/wiki/Pagina_principale),l'HTML (<< l'HyperText Markup Language>>), è un linguaggio che viene utilizzato principalmente per il disaccoppiamento della struttura logica di una pagina web.

[471] Si cita, ad es. : Li, *Cacciatori di bug. Guida per imparare a trovare e riportarevulnerabilitàweb*,Apogeo,2023; Sinha, *Bug Bounty Hunting for Web Security: Find and Exploit Vulnerabilities in Web sites and Applications*, APress,2019.

[472] Pica, *op.cit.,* pag. 455.

[473]Pascuzzi, *op. cit.,* pagg.93-94 definisce i cookies come << file di piccole dimensioni, normalmente in formato Ascii, che contengono informazioni di base relative a un utente in relazione a un server >>.

[474]Come indicato da Pascuzzi, *op. cit*., pag.95, la disciplina dei cookies è posta dall'art. 30 del Regolamento UE 2016/679 in Gazzetta Ufficiale dell'Unione Europea del 04/05/2016.

[475] Pica, *op.cit.,* pag. 456.

[476]Sulla base de: Libro verde sulla convergenza tra i settori delle telecomunicazioni, dell'audiovisivo e delle tecnologie dell'informazione e sulle sue implicazioni normative, COM(97) 623; il termine "convergenza" viene di solito indicato come, alternativamente:
a) <<la capacità di differenti piattaforme di rete di gestire servizi di tipo fondamentalmente simile, b) l'unificazione di apparecchiature di largo consumo (ad es., telefono, televisione e computer) >>.

- Infine, bisogna guardare ai programmi <<trojan>> (conosciuti anche come <<cavallo di Troia>>), che permettono di <<accedere a dati e ad attività del […] computer per via telematica>>[477], assumendo il dominio assoluto del sistema informatico della vittima- che non può far altro se non interrompere la connessione e riparare poi i danni.
  L'acquisizione di informazioni può avvenire in due modalità: o tramite appositi programmi (i c.d. <<packet sniffers>>),oppure tramite softwares (i c.d. <<softwares trojans>>) volti all'intercettazione di dati da sistema remoto. Questo è il classico strumento utilizzato per qualsiasi accesso abusivo (punibile ex art. 615- ter c.p.), e frequentemente sono ardui da individuare.

  Si accenna anche al fatto che il trojan - secondo alcuni autori[478]-viene incluso nella categoria del <<virus informatico>>[479], assieme ai c.d. <<worm>> e alle <<logic bombs>>[480].
  In base al loro contenuto, questi virus informatici possono avere effetti diversi, ma comunque tutti gravi: oltre all'accesso abusivo già accennato, basta menzionare l'alterazione del contenuto di files e di programmi nel sistema, la <<sostituzione di funzioni>>[481], nonché il produrre interferenze che impediscano il normale funzionamento del sistema, fino ad arrivare alla completa distruzione di esso.

  Ora, quale può essere uno mezzo difensivo contro gli strumenti summenzionati? È ardua una risposta a questa domanda: si è ipotizzato come soluzione la navigazione in rete in anonimato[482] e la crittografia[483]. Senza soffermarsi sulla questione della tutela dei dati

---

[477]Pica, *op. cit.,*pag.456.

[478] Si cita: Parodi e Calice, *Responsabilità penali ed Internet. Le ipotesi di responsabilità penale nell'uso dell'informatica e della telematica*,Il Sole 24 Ore, collana Diritto,2001.

[479]Come indicato da: Ziccardi*, I virus informatici: aspetti tecnici e giuridici*, in Ciberspazio e Diritto, 2001, Vol.2, n.3-4, pag. 352, i virus informatici sono programmi di vario contenuto, <<composti da una parte destinata alla riproduzione e da un'altra che deve garantire funzionalità distruttive o di disturbo>>. Si deduce dunque che le caratteristiche di questi virus sono <<la capacità di autoriprodursi>>nel sistema ed infettare altri programmi, nonché la capacità di danneggiamento del sistema informatico.

[480]La definizione di entrambi si ritrova in: Ziccardi, *op. cit*., pag. 352. I <<worm>> sarebbero infatti dei <<programmi che si riproducono incessantemente all'interno dell'elaboratore>>, bloccando così il normale funzionamento del sistema.
Le <<logic bombs>> invece sono programmi aventi al loro interno <<una funzione diretta a danneggiare o a impedire il funzionamento del sistema>>. Esse si attivano o immediatamente alla loro introduzione nel sistema, oppure in un momento successivo, prestabilito dal loro autore.

[481]Ziccardi, *op. cit*., pag. 352.

[482] Sulla base dell'art.4 del Regolamento UE 679/2016, per<<dato personale>> s'intende<<qualsiasi informazione riguardante una persona fisica identificata o identificabile
(intendendo per <<identificabile>><<la persona fisica che può essere identificata, direttamente o indirettamente>> tramite una serie di elementi, es. <<un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale>>). Conseguentemente, riprendendo l'art.2, lett. a) della direttiva 95/46/CE (abrogata dal suddetto regolamento)

personali nella dimensione cibernetica[484], si sono sollevati dubbi sulla liceità di entrambi gli strumenti, dato che entrambi, per altro verso, agevolerebbero alla commissione dei reati cibernetici ed informatici, nascondendo l'identità dei loro autori.

Non si vuole negare in questa sede che l'identità digitale non sia stata mai attaccata nello spazio cibernetico (anzi, è stata spesso definita negli studi più recenti come <<vulnerabile>>[485]), ma – come sottolineato da numerosi autori- arrivare *in extremis* a censurare l'anonimato in *toto* perché illecito è di carattere eccessivo: oltre al fatto che il dato non è anonimo in assoluto, ma <<può essere reso anonimo in determinati contesti e per alcuni scopi>>[486], la liceità o illiceità del dato anonimo dipende dalle finalità che si intendono perseguire. Impedire del tutto l'anonimato non comporterebbe dunque la diminuzione della commissione di illeciti, quanto piuttosto <<il solo effetto di lasciare del tutto indifesi milioni di utenti di fronte allo strapotere delle organizzazioni economiche, e prive di riservatezza le comunicazioni aziendali e professionali>>[487]. Inoltre, l'anonimato rappresenta odiernamente uno degli strumenti che permette la libera manifestazione del pensiero e della personalità, <<proprio per la maggior sicurezza -quantomeno percepita- di non esser identificati>>.[488]

Da questo si permette di dedurre l'approccio <<neutro>> degli strumenti presenti in Rete: la liceità o illiceità dipende dalle modalità e finalità per cui vengono utilizzate (come si vedrà in seguito anche per la piattaforma IRC[489]).

---

il dato anonimo è quel dato che <<in origine, o a seguito di trattamento>>, non può esser associato ad alcuna persona identificata o identificabile.

[483] Secondo la definizionedi Pascuzzi,*op. cit*,pag. 47, la crittografia è una tecnica posta allo scopo di <<convertire dati leggibili e comprensibili in dati illeggibili e incomprensibili usando un algoritmo di cifratura e una chiave>>, in modo da consentire la comprensione delle informazioni solo a chi è a conoscenza dell'algoritmo e/o in possesso della chiave.

[484] Per ulteriori approfondimenti sul punto, si fa riferimento a: Picotti, *Il diritto penale dell'informatica nell'epoca di Internet,*pagg.173-300, Eusebi, *op. cit.,* in *Ciberspazio e diritto*, 2013, vol.14, n.48 (2-2013), pagg. 183-209;Tosi (a cura di), *Privacy digitale : riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè, 2019; Pascuzzi, *op.cit.,* pagg.71-114, Ortalda e Leucci, *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Riv.it. inf. e dir.,* 2022, fasc.4, pagg.145-155.

[485] Brighi e Di Tano, *Identità, anonimato e condotte antisociali in Rete. Riflessioni informatico-giuridiche*, in *Riv. Fil. Dir*., 2019, fasc. 1, pagg. 188. In particolare, oltre alla difficoltà della tecnologia di avere strumenti d'accertamento efficaci per la corrispondenza tra identità fisica e digitale, emerge come i dati personali siano sempre più oggetto di numerose condotte illecite (in particolare, col c.d. <<furto dell'identità digitale>>), nonché la crescente tendenza <<a far circolare le proprie informazioni personali in ambienti erroneamente percepiti come privati>>.
Si veda anche: Cass.Pen., sez. V, n. 46674/2007 in *Dir. Int*., n.3/2008,,pagg. 249-252.

[486] Brighi e Di Tano*,op. cit*., pag. 190. Nello stesso senso: Eusebi, *op. cit.,* pag. 184,

[487] Pica,*op.cit., pag. 458.*Nello stesso senso (seppur incentrato più sui reati d'odio): Scorza, *In difesa dell'anonimato online. I leoni da tastiera non si battono eliminandolo*, in HuffPost dell'11/12/2022 (https://www.huffingtonpost.it/)

[488] Brighi e Di Tano, *op. cit*., pag. 194.

[489] Si fa diretto richiamo al Capitolo III, punto 2.2.

In chiusura, non solo si trae come gli innumerevoli strumenti per il tracciamento illecito di dati variano in base alla tipologia di reati che l'autore intende commettere; ma si ha anche un'ulteriore conferma di come l'intero sistema del cybercrime non possa essere inquadrato incategorie tassative, in ragione della vastità del cyberspazio stesso.

1.3. Il superamento della "via unidirezionale del web": un cenno generale ai profili criminologici degli autori e delle vittime dei reati cibernetici .

Ultimo aspetto importante da considerare per la trattazione in generaledel fenomeno del Cybercrimeè il c.d. <<superamento della via unidirezionale del web>>[490] : grazie alla nascita del Ciberspazio, l'utente passa ad essere -da mero destinatario passivo di informazioni- non solo soggetto attivo nelle relazioni che si intrecciano nel Ciberspazio, ma diventa anche<<merce>>[491] da cui estrapolare – per scopi leciti o meno- informazioni di ogni tipo (es. sulle tendenze o sulle preferenze dell'utente nella navigazione dei siti Internet).

In sintesi, se da un lato << la personalità di ciascun individuo è radicalmente "potenziata" nelle sue capacità di esprimersi, comunicare, [….]>>, allo stesso tempo essa è però << esposta ad un "prelievo" sistematico di dati,[…] tracce, aggressioni, che possono condizionarla, soggiogarla [….] nelle relazioni che vi si svolgono e di cui diviene […] parte integrante, tanto da non potervisi sottrarre, se non violando i limiti di legittimazione della sua "appartenenza" al *cyberspace*>>[492].

È necessario premettere chenon si può tracciare un profilo criminologico generale ed al contempo specifico né per l'autore né per la vittima di questi reati (a meno che l'oggetto di studio non sia incentrato su una specifica tipologia di reato cibernetico o informatico), a causa dell'immenso numero di tipologie di vittime e autorie della potenziale vastità delle modalità di manifestazionedi questi reati, nonché dellaloro costante mutazione.

[490]Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme,*cit., pag.55.
[491]Picotti, *op. ult. cit.*, pag.56.
[492]*Ivi*, pag.57.

Ad ogni modo, ci si sforzerà di elencare quali siano, in via del tutto generale, le tendenze ed i tratti caratteristici riguardo siail profilo dell'autore che quello della vittima da un punto di vista criminologico[493].

Questo è possibilegrazie ad una serie di elementi che accomunano i crimini sia informatici che cibernetici e che, allo stesso tempo, li differenziano dai reati <<tradizionali>>:

- <<l'assenza di contatto fisico e reale tra autore e vittima>>[494],
- Un' enorme velocità nell'eseguire e replicarela condotta criminosa,
- La <<dissociazione tra identità virtuale e digitale>>[495], in seguito alla possibilità di creare in Rete una o più identità digitali con informazioni non corrispondenti a quelle appartenenti alla identità personale (in certi casi, anche senza alcuna informazione personale),
- La già citata capacità di anonimato dei soggetti agenti, che - assieme agli elementi precedenti- rende particolarmente complessa la loro individuazione (nonché la successivaapplicazione di misure sanzionatorie rispetto alle loro condotte),
- La c.d. <<aterritorialità della Rete>>, intesa come <<disancoraggio delle attività svolte sulla Rete da uno spazio fisico ben definito>>[496], che rendedunque l'azione dell'agente estendibile ad una dimensione globale, superando i confini territoriali dello Stato in cui eglisi trova fisicamente;
- Una grande difficoltà con riguardo all'armonizzazione delle norme di diritto penalea livello internazionale relative alla tematica[497] e le difficoltà operative di collaborazione tra forze di polizia di differenti paesi nelle attività d'indagine,
- L'assenza sia di soggetti terzi intermediari nella rete in grado di intervenire nella repressione e prevenzione di possibili abusi online (fatto salvo il caso degli ISP, i c.d.<<Internet Service Providers>>, la cui responsabilità penale è limitata e comunque discussa [498]), nonché dei c.d. <<gatekeepers>> (<<guardiani>> in inglese), ossia

[493]Per maggiori approfondimenti: Balloni et al., *Criminologia Applicata*, CEDAM, 2019, pagg. 311 e ss.

[494]Scirpa, *Cybercrime e criminalprofiling: i nuovi approcci delle tecniche investigative nell'era tecnologica*, in Ciberspazio e Diritto, vol. 20, n.62 (1-2 /2019), pag.305. Nello stesso senso: Apruzzese, *Autori e vittime nella criminalità informatica,* in *Rivista Quadrimestrale di Criminologia, Vittimologia e Sicurezza,* 2009/2010, Vol. 3 e 4, numeri 3 e , pag.105.

[495]Bussolati, *L'associazione per delinquere <<informatica>>,* in AA. VV., Cybercrime, (a cura di) Cadoppi, Canestrari, Manna, Papa,2019, UTET Giuridica, a pag. 256, fa in particolare riferimento a: Suler, *The online dishinibition effect*., in *Cyberpsycology & Behaviour,*2004, Vol.7, Issue 3, pagg. 321-326.

[496]Pascuzzi,*op. cit*., pag. 348. Riguardo un 'altra accezione del concetto di aterritorialità, comportante la difficoltà dell'individuazione della disciplina giuridica da applicare ai rapporti presenti nel cyberspazio, si veda la nota sopra relativa alla c.d. <<autoregolazione>> del Web.

[497]Riguardo a questo profilo, si fa rinvio al paragrafo 2.2.

[498] Senza approfondire ulteriormente sul tema, si segnala la presenza di non pochi dibattiti in dottrina ed in giurisprudenza su questa figura, soprattutto sui fondamenti ed i limiti di una responsabilità penale della stessa per i contenuti illeciti pubblicati da terzi: peraltro, allo stato,in base al quadro normativo offerto dal D.lgs. n.

<<tecnologie e/o persone tecnologicamente preparate>>in grado di poter svolgere una effettiva protezione del bene giuridico d'interesse dell'autore del reato[499],

- La generale disinformazione delle vittime sulla materia tecnologica, informatica e/o cibernetica, nonché la loro poca consapevolezza di divenire effettivamente tali.

Come è possibile percepire intuitivamente, tutti questi fattori non solo hanno contribuito (se non pure aumentato) la commissione dei reati informatici e cibernetici, ma permettono anche di comprendere meglio il quadro che si andrà a tracciare sia sugli autori che sulle vittime dei reati cibernetici, nonché renderà forse possibile ritrovare delle differenze tra queste e le tipologie di reati <<tradizionali>>.

1.3.1. La vittima dei cybercrimes: caratteri e tipologie.

Partendo dalla figura della vittima, si è riscontrato quanto sia particolarmente arduo darneun profilo completo e generale per tutta una serie di fattori:*in primis*, il fatto che gli studi e le ricerche di criminologia e psicologia sul tema sono di carattere piuttosto recente e di frequente piuttosto focalizzati su una tipologia specifica di reato cibernetico, nonché il rischio(come sottolineato da alcuni studiosi)[500] che l'utilizzo dei risultati, ottenuti dalle

---

70/20035 (di recepimento della cd. Direttiva *e-commerce*) e, in particolare dagli artt. 16 e 17 ivi contenuti e alla relativa interpretazione giurisprudenziale, pare comunque esclusa la configurabilità di una responsabilità da reato omissivo improprio per non aver impedito il reato altrui. Per maggiori approfondimenti, si cita: Per la dottrina, Picotti, *Diritto Penale e tecnologie informatiche: una visione d'insieme*, in Picotti et al., *Cybercrime*, pagg.81-89; Fornasari, *Il ruolo della esigibilità nella definizione della responsabilità penale del Provider,* in Picotti, *Il diritto penale dell'informatica nell'epoca di Internet*, pagg. 423-433; Pascuzzi, *op.cit*., pagg. 309-314.
Per la Giurisprudenza, si fa riferimento a: Tribunale, Milano, sez. IV, n.1972/2010 (il caso <<Google -Vivi Down>>), con note di : Catullo, *Ai confini della responsabilità penale: che colpa attribuire a Google*, in *Giur. Merito*, 2011 fasc.1, pagg. 0159B e ss.; Franceschelli, *Sul controllo preventivo del contenuto dei video immessi in rete e i provider. A proposito del caso Google/Vivi Down.,* in*Riv. Dir. Ind*., fasc.4-5, 2010, pagg. 347 e ss.

[499]Tonellotto, *op. cit.,* pag. 9, fa in particolare riferimento alla teoria di Cohen e Felson, la c.d. <<Teoria delle attività routiniarie>> (indicata in : Cohen and Felson, *Social change and crime rate trends: A routine activity approach*, in *American Sociological Review*, 1979, vol.44(4),pagg. 588 – 608). Secondo questa teoria, un crimine si realizzerebbe quando sono presenti contemporaneamente tre elementi: un aggressore motivato; un <<bersaglio appetibile>> (ossia un bene o una persona da aggredire); nonché l'assenza di un guardiano ovvero l'incapacità dei presenti di prevenire che il crimine accada.
Oltre all'ammissibilità dell'applicazione della teoria anche nel Cyberspazio, l'Autore nota, *op. cit.,* a pag.9, come queste tre condizioni si verifichino molto frequentemente nei reati informatici: se si considera come oggetto d'interesse del criminale il <<dato informatico>> (inteso sia come <<singolo elemento computazionale che incorpora in sé il valore stesso dell'informazione, […], ma anche come porzione di codice sorgente, software, che consente la gestione di dispositivi connessi alla rete>>), è chiaro che la stessa assenza di un possibile <<custode>>del dato informatico stesso contribuisca alla consumazione di reati informatici.

[500]Hoff-de Goede, Leukfeldt, Kleij, Weijer, *The Online Behaviour and Victimization Study: The Development of an Experimental Research Instrument for Measuring and Explaining Online Behaviour and Cybercrime*

diverse ricerchee tramite diverse metodologie, diano vita ad un profilo criminologico di carattere eccessivamente contraddittorio.

Ad ogni modo, prima di procedere oltre, è necessario eseguire un'importante premessa sulla tematica in questione: il quantitativo di persone che odiernamente hanno effettivamente denunciato di essere vittime di cybercrime è piuttosto basso, addirittura si parla di una problematica nella <<misurazione del crimine sconosciuto>>[501]. Numerosi studiosi e ricercatori[502] indicano che tutt'oggi il numero di vittime di cybercrime attestate nel mondo è parziale: sono moltissime sia le persone che non si rendono conto di esser divenute vittime[503], sia quelle che, pur acquisendo la consapevolezza di esser divenute vittime, decidono di non denunciare il reato[504].

Questa rinuncia alla segnalazione del fatto può avvenire per diverse motivazioni, di cui si segnalano in seguito le più comuni:

- Talvolta la scelta di non denunciare è dovuta ad una scelta di strategia aziendale: una volta subita la condotta criminosa, l'impresa tende a far tacere tutto o per evitare che la sua stessa immagine aziendale venga rovinata se si venisse a sapere che essa ha subito violazioni, ovvero su indicazione dei consulenti finanziari ed informatici, che suggeriscono di risolvere la questione internamente[505];
- Secondo un apposito studio in Regno Unito[506]la scelta di non denunciare è strettamente collegata alla gravità dei danni psicologici ed economici arrecati alla vittima in seguito al reato: nel caso in cui i danni (psicologici, fisici, emotivi, economici) non siano di grande

---

Victimization, in Kranenbarg, Leukfeldt, *Cybercrime in context: The human factor in victimization, offending and policing*, 2021,Springer International Publishing AG, pag. 22.

[501]In inglese, <<measurement of unknwon crime>>: Reep-van den Bergh, Junger, *Victims of cybercrime in Europe: a report of victim surveys*, in *Crime Science,* 2018, Volume 7, pag.12.

[502]Citando alcuni esempi: De Vivo, Ricci; *Diritto,Crimini e tecnologie*, in Informatica e diritto, XXXVIII Annata, Vol. XXI, 2012, n. 2, pag. 55; Koops, *The Internet and its Opportunites of Cybercrime*, in AA.VV., *Transnational Criminology Manual*, (a cura di) Herzog-Evans, Vol.1, Wolf Legal Publishers, 2010, pag. 742.

[503]Citando alcuni esempi: Reep van-derBergh, Junger, *op. cit.*, pag. 11;Henson, Reyns, Fisher, *op. cit*., pag. 561.

[504] Si riporta in: Goucher, *Being a cybercrimevictim,* in Computer Fraud& Security, 2010, Issue 10, pagg. 16-17, che nella ricerca del 2010 condotta da Norton (<<Cybercrime report: the human factor>>, cit., http://www.norton.com/cybercrimereport/), delle 77.000 persone intervistate nel mondo, il 65% aveva dichiarato di esser stato vittima di un reato cibernetico, ma solo il 44% aveva deciso di denunciare il reato alla polizia.

[505]De Vivo, Ricci, *op.cit*., pag. 55.

[506]Button, Blackbourn, Sugiura, Shepherd, Kapend, Wang, *Victims of Cybercrime: Understanding the impact through accounts*, in Kranenbarg, Leukfeldt *Cybercrime in context: The human factor in victimization, offending and policing*, (a cura di), Springer International Publishing AG, 2021,pag.145; nonché, riguardoallecategoriedeireati cybernetici divisi in base all'impatto sulla vittima, si richiama Id., *op. cit*., pag. 141.

entità, spesso le vittime additano l'avvenimento più come una <<sfortuna>> che come un effettivo danno (o violazione) da loro subita;

- Sempre riguardo le tipologie di reati cibernetici che hanno arrecato un danno di entità lieve-media, può esserci alla base della scelta delle vittime un'analisi preventiva di bilancio costi-guadagni: sia il fatto che un eventuale processo avviato contro l'autore del reato - sempre se sia stato possibile identificarlo[507]- comporterebbe un'enorme spendita di tempo e denaro (poiché esso si potrebbe potenzialmente svolgere in un paese diverso da quello della vittima), sia la difficoltà di ottenere prove a sostegno della posizione della vittima, fanno spesso ritenere a quest'ultima che instaurare un'azione penale sarebbe solo una mera perdita di tempo[508], inducendola dunque a rinunciare a segnalare l'avvenimento;
- Altro motivo che potrebbe far decidere alla vittima di non denunciare è di carattere psicologico: spesso, le vittime si sentono in colpa per esser state così <<stupide>> ad aver tenuto un comportamento che ha consentito la commissione del reato nei loro confronti; perciò, sentendosi in parte responsabili per quello che è successo, ritengono di non dover meritare nessun aiuto[509];
- Ultima ragione- ma non meno importante è la sfiducia nelle capacità delle banche (se il bene leso dalla condotta criminale è stato il denaro)e della polizia di disporre dei mezzi e strumenti necessari per garantire loro tutela: considerata l'infinitesimale possibilità di riuscire ad individuare l'autore del reato, vi è la concreta possibilità che non vi possa esser alcuna azione giudiziaria, una condanna ed in seguito il risarcimento a favore della vittima.
  Conseguentemente, nei casi in cui il danno subito sia stato di carattere lieve, tutto questo comporterebbe <<solo>> il rischio che la vittima venga additata dagli altri come sciocca, non in grado di resistere alle tentazioni [510]; nei casi più gravi invece si è dimostrato che il fallimento della giustizia o del supporto cercato aggravino le condizioni di isolamento della vittima e la sua situazione emotiva e psicologica[511].
  Per cui, mettendosi nei panni di quest'ultima - perché agire <<per niente>>, se in seguito si otterrebbero ulteriori danni oltre a quelli già subiti?

Procedendo ad una descrizione più dettagliata del profilo della vittima, è importante precisare che in un esperimento eseguito sulla base della teoria delle attività routinarie

[507]Goucher, *op. cit*., pag. 17.
[508]*Ibidem.*
[509]*Ibidem.*
[510]*Ibidem.*
[511]Button, Blackbourn, Sugiura, Shepherd, Kapend, Wang, *op. cit.* , pag. 154.

sopracitata[512], prendendo alcune variabili fisse (età, genere, livello di educazione e stato civile),si è dimostrato che nei crimini tradizionali in media le vittime sono tendenzialmente giovani maschi, con un basso livello di istruzione e con la tendenza a trascorrere del tempo all'aperto[513].

Inoltre, con riguardo alla vittima dei crimini tradizionali (in particolare, quelli caratterizzati da violenza o minaccia da parte dell'agente nei confronti del soggetto passivo), spesso si riscontrano due caratteristiche fondamentali, ossia il contatto fisico tra vittima e autore, e la creazione per la vittima di forti sentimenti di paura e di senso del pericolo.[514]

A questa figura della vittima tradizionale si contrappone quella della vittima del cyberspazio: nonostante anch'essa (al pari della vittima nel reato tradizionale) percepisca la paura ed il pericolo, in realtà chiunque faccia utilizzo della tecnologia informatica è una potenziale vittima, a prescindere da <<l'età, la cultura, la professione o le abitudini sessuali, criteri questi che influiscono grandemente nella potenziale vittima dei reati comuni>>[515].

A supporto di quanto detto finora vi sarebbero alcuni studi condotti in Olanda, secondo i quali le vittime di cybercrime sono molto più simili alla figura del<<cittadino medio rispetto alle vittime della criminalità tradizionale>> [516], rilevando appunto come la condizione di vittima in questo contesto sia trasversale al genere e all'età, in base alla situazione socio-economica e alle condizioni in cui si trova. È proprio in questo stesso studio che si parla della <<teoria di normalizzazione delle vittime di cybercrime>>[517]: considerato che i computer ormai sono oggetti posseduti da chiunque nel mondo e tutti

---

[512]Sulla base della teoria di Cohen e Felson, *op. cit.,*più le persone eseguono attività quotidiane in assenza di <<guardiani>>, nonché in luoghi pieni di potenziali offensori, aumenta la percentuale di rischio della persona di diventare vittima.

[513] Tonellotto*, op. cit.,* pag. 13 fa riferimento alle ricerche ottenute da: Bunch, Clay-Warner, Lei*, Demographic characteristics and victimization risk: Testing the mediating effects of routine activities,* in *Crime & Delinquency*, 2015, Vol.61, Issue 9, pagg.1192-1195, i quail sono giunti a queste conclusioni analizzando i dati personali delle vittime americane del 199 aventi subito lesioni ovvero rapina . Nello stesso senso: Lauritsen, Sampson, Laub, *The link between offending and victimization among adolescents*, *cit.,* in *Criminology*, 1991, vol. 29, Issue 2, pagg. 264-292 (https://doi.org/10.1111/j.1745-9125.1991.tb01067.x/).

[514]Henson, Reyns, Fisher *Cybercrime Victimization*, in Cuevas, Rennison, *The Wiley Handbook on the Psychology of Violence*, Wiley Blackwell, 2016, pag. 556.

[515]De Vivo, Ricci, *op. cit*., pag. 58. *Contra:* Grabosky, *Virtual Criminality: Oldwine in new bottles?,* in *Social & Legal Studies,* 2001, Volume 10, Issue 2, (https://doi.org/10.1177/a017405). Seppur egli riconosca che il numero di reati cibernetici stia crescendo sempre più (e, di conseguenza, anche le modalità in cui si può colpire una vittima), egli identifica a pag. 248 che in realtà la criminalità virtuale non è altro se non <<vecchio vino in nuove bottiglie >> (<<oldwine in new bottles>>): seppur si manifesta in maniera diversa, è sempre un crimine a cui si possono tranquillamente applicare le medesime teorie e i principi della criminologia tradizionale.

[516] Junger, Montoya, Hartel, Heydari,*Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe, i*n *International Conference On Cyber Situational Awareness, Data Analytics And Assessment,* London, UK, 2017, pag.7. DOI: 10.1109/CyberSA.2017.8073391/.

[517]*Ibidem.*

tendenzialmente trascorrono molto tempo su internet, qualunque soggettoperciò potrebbe diventare vittima.

Qui dunque si scorge una palese differenza rispetto ai crimini tradizionali: mancando il contatto fisico tra autore e vittima di un reato cibernetico o informatico, difficilmente l'offensore ha come obiettivo quello di colpire con la sua condotta una specifica vittima, nonché una vittima che effettivamente conosca nella vita *offline* (salvo in casi particolari, ad es. quando l'autore del reato aveva già precedentemente eseguito altre condotte criminosecontro la vittima *off-line*,come ad es., atti di bullismo e poi di cyberbullismo verso la medesima persona, o comunque casi in cui sussisteva già un rapporto con quella particolare vittima).

Piuttosto, non solo il contatto tra sconosciuti è spesso dovuto ad una <<violazione del domicilio virtuale>>[518] da parte dell'autore del reato, ma anche ci sarebbespessol'interesse di colpire un insieme indeterminato di persone, legato da interessi comuni, ovvero che si ritrovi in circostanze <<che li rendono bersaglio o oggetto di vittimizzazione>> [519]. Pertanto, seppur in questo paragrafosi parlerà della vittima al singolare, bisognerà tenere presente che nella fenomenologia del cybercrime non esiste solo la figura della vittima singola - che, si ripete, rimane di carattere minoritario - : ad essa si deve necessariamente affiancare la figura della c.d. <<vittima collettiva>>[520].

C'è poi un'altra differenza importante da tenere in considerazione rispetto alla criminologia tradizionale. Nell'analisi del profilo vittimologico non ci si può solo soffermare sul soggetto vittima di un crimine cibernetico/informatico, ma bisogna eseguire un confronto costante tra questa figura e, nell'ordine: il soggetto che non è mai stato vittima di reato, i soggetti che sono state vittime solo di crimini *off-line*, quelli che sono stati precedentemente vittime di crimini *off-line* e poi *online*, quelle che sono state più volte vittime di crimini cibernetici e/o informatici (è il caso della c.d.<<*repetitive victimization*>>[521]).

---

[518]Marotta, *Tecnologie dell'informazione e nuovi processi di vittimizzazione,* in *RivistaQuadrimestrale di Criminologia, Vittimologia e Sicurezza,* 2012, Vol. VI , n.2 , pag. 101.

[519]De Vivo, Ricci, *op. cit*. ,pag. 58.

[520]*Ivi*, pag. 55, fan riferimento per la definizione di vittima collettiva (<<gruppi di individui uniti da speciali legami, interessi o fattori di circostanze che li rendono bersaglio o oggetto di vittimizzazione>>) a : Fedeli, Ricci, Cortucci, *Lineamenti di Criminologia,cit.,* Edizioni Scientifiche Italiane, 2006, pag. 163 e ss.

[521] Per maggiori approfondimenti sul punto, si cita: Fagan, Mazerolle, *Repeat Offending and Repeat Victimization: Assessing Similarities and Differences* in *Psychosocial Risk Factors*; in *Crime & Delinquency*, 2011, Vol.57, Issue 5, pagg.732–755 (DOI: https://doi.org/10.1177/0011128708321322);

Questo per quale motivo? È stato dimostrato come, tra questi quattro gruppi, le ripercussioni psicologiche ed emotive (es. la paura di rimanere nuovamente vittima, il senso della propria sicurezza personale) siano molto più forti per l'ultimo gruppo rispetto alla persona che è stata vittima di cybercrime un'unica volta, poiché in essi si manifestano maggiori difficoltà nell'affrontare le ripercussioni di carattere emotivo e psicologico derivanti dalla condotta illecita[522].

Fatte queste considerazioni generali sul profilo della vittima, si delineeranno adessoi tratti della personalità della vittima, nonché quali sarebbero i fattori in grado di far aumentare il rischio di vittimizzazione nel cybercrime, guardando alcunerecenti ricerche psicologiche e criminologiche.

Nel tentativo di individuare quale risulterebbe esser la personalità del soggetto che ha alti livelli di probabilità di divenire vittima di questa tipologia di reati, bisogna anzitutto richiamare all'attenzione due importanti teorie. La prima teoria da tenere in considerazione è quella delle cinque dimensioni della personalità (c.d. <<Big Fivetheory>>[523]): il carattere d'ogni essere umano è definito da cinque tratti: estroversione, gradevolezza, apertura mentale, coscienziosità e nevroticismo[524].

Turanovic, Pratt, "*Can't Stop, Won't Stop'': Self-Control, Risky Lifestyles, and Repeat Victimization,* in *Journal of quantitative criminology,* 2014, Vol.30, Issue 1, p.29-56 (DOI:10.1007/s10940-012-9188-4/).
Si accenna al fatto che, in entrambe le opere sovra citate si tende ad accogliere la teoria di:Schreck et al. , *Self-Control, Victimization, and Their Influence on Risky Lifestyles: A Longitudinal Analysis Using Panel Data*, in *Journal of Quantitative Criminology*, vol. 22, n.4, 2006, pagg. 319–340 (DOI: https://doi.org/10.1007/s10940-006-9014-y/), secondo cui, sullo studio di vittime subenti violenza fisica,furto o rapina e sulla base della teoria delle attività routinarie, chi manifesta un comportamento rischioso (es. abuso di sostanze, passare il proprio tempo in attività sociali non particolarmente supervisionate, eseguire condotte offensive)e ha poco autocontrollo, ha una maggiore possibilità di ricadere vittima di reato.Si deve però precisare che , rientrare nella vittimizzazione ripetuta non dipende unicamente dal comportamento dell'offeso. Visto che la vittimizzazione ripetuta si manifesta in seguito a più condotte illecite dell'autore la cui pericolosità viene ignorata o sottovalutata, spesso la vittima, in seguito ad un probabile legame emotivo con l'autore dei reati, ma anche avendo subito da parte dall'autore intimidazioni o ad altre forme di violenza fisica o psicologica, si mette nella posizione del mero subire per paura, angoscia, senso di colpa – dovuto anche ad un maggior isolamento della vittima, creato spesso dall'offensore. Inoltre, spesso la vittimizzazione reitarata può essere anche dovuta ad una negligenza o scarsa attenzione degli operatori sociali nella fase successiva alla consumazione del primo delitto. Un caso classico è la violenza domestica subita dalle donne in Italia. Per maggiori approfondimenti: Balloni et al.,*op. cit*., pag. 386;De Luca, *Vittimologia e Prevenzione. La percezione femminile di essere vittime*, in Den Cataldo Neuburger et al., *Anatomia del crimine in Italia : manuale di criminologia*., Giuffrè, 2013, pagg.1073 e ss. .

[522]Virtanen, *Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities,* in *Psychiatry, Psychology and Law*, 2017, vol.24, Issue 3, pag.326 (DOI: 10.1080/13218719.2017.1315785); ma si veda anche:Popham, *Assessing the Detrimental Impact of Cyber-Victimization on Self-Perceived Community Safety*,cit., in AA.VV., *Cybercrime in context: the Human factor*, pagg.103 e ss.

[523]Si fa riferimentoallateoria diMcCrae, Costa*, A Five-Factor theory of personality,* in Pervin& John, *Handbook of personality: Theory and research*, 1999, Secondaedizione, Guilford Press, pagg. 139-153.

[524] Dandone una breve definizione:

- l'Apertura Mentale (*Openness*) indica la curiosità e ricerca di nuove esperienze o attività fuori della routine quotidiana- chi risulta aver livelli bassi di questo tratto, è una persona più realista e tradizionalista, nonché poco creativa.

La seconda, di carattere sociologico- a differenza della precedente-, viene definita la c.d. <<teoria dell'autocontrollo>> [525]. Nel cercare di capire perché determinati individui diventano criminali ed altri no, secondo questa teoria non esiste una categoria di soggetti più propensa a commettere reato piuttosto di altre, ma tutto si basa sulla capacità del soggetto di resistere alle proprie pulsioni egoistiche del momento- aspetto che si impara nella propria infanzia, grazie all'ambiente sociale dato dalla famiglia e dalla scuola. Seguendo il ragionamento, l'individuo che ha bassi livelli d'autocontrollo manifesta la tendenza a rispondere in modo immediato agli stimoli dell'ambiente, avendo un atteggiamento del <<qui ed ora>>, senza dunque tenere in considerazione quali potrebbero esser le conseguenze delle proprie azioni: tutto ciò non rende l'individuo solo più propenso a commettere un reato, ma anche più predispostoa poter subire un reato[526]. Questo tratto dell'autocontrollo può esser considerato incluso nel tratto della coscienziosità della teoria menzionata prima[527].

Sulla base di queste due teorie, sarebbe possibile ricostruire sia il quadro della vittima tradizionale che quello della vittima del cybercrime. Se la prima sarebbe caratterizzata da un carattere con poco autocontrollo, uno stile di vita con attività di carattere rischioso, nonché fattori socio-demografici che aumentino la probabilità di esser vittima[528] (es. frequentare quartieri poco raccomandabili); bisogna vedere, guardando gli studi e gli esperimenti eseguiti[529], se corrispondono le stesse caratteristiche per la personalità della vittima di cybercrime.

- La Coscienziosità (*Concentiousness*) rappresenta la capacità di organizzazione, perseveranza e motivazione nel raggiungimento degli obiettivi: chi ha livelli alti in questo tratto è una persona disciplinata e scrupolosa - al polo opposto, si trova la pigrizia, l'indisciplinatezza e l'incuranza.
- L'Estroversione (*Extroversion*)indica il grado di soddisfacimento che l'individuo trae dalle relazioni interpersonali – se la persona ha livelli bassi in quest'aspetto, sarà una persona più introversa.
- La Gradevolezza (*Agreeablness)* individua il livello di empatia, altruismo e cooperatività - chi ha livelli bassi su quest'elemento, sarà una persona cinica, rude, sospettosa, vendicativa, manipolatrice o ostile.
- Infine, il Nevroticismo (*Neuroticism*) guarda all'instabilità emotiva: chi ha livelli positivi in questo tratto è tendente alla ruminazione, è una persona nervosa ed insicura, emotiva, tendente all'ansia e/o alla depressione. Chi ha livelli negativi è invece una persona stabile emotivamente, soddisfatta di sé e sicura.

[525]La teoriasiritrova in: Gottfredson, Hirschi, *A general theory of crime,*1990, Stanford University Press.

[526]Si cita, sulpunto:Bossler, Adam, Holt, *The Effect of Self-Control on Victimization in the Cyberworld,.* in *Journal of Criminal Justice*, 2010, vol. 38, Issue 3, pagg. 227-236 doi: 10.1016/j.jcrimjus.2010.03.001/ .

[527]Van de Weijer, Leukfeldt, *Big Five Personality Traits of Cybercrime Victims*, in *Cyberpsychology, Behaviour, and Social Networking,* 2017, Vol.20, Issue 7, pagg. 410.DOI:10.1089/cyber.2017.0028/.

[528]Göttker, op. cit., pag. 4, fa riferimento a:Kranenbarg, Holt, van Gelder, *Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap*, in *Deviant Behavior*, 2019, Vol.40, Issue 1, pag.40-55. doi:10.1080/01639625.2017.1411030/

[529]Si farà in particolareriferimento a: Göttker, *op.cit.,*pagg. 14-17; Van de Weijer, Leukfeldt, *Big Five Personality Traits of Cybercrime Victims*, in *Cyberpsychology, Behaviour, and Social Networking,* 2017, Vol.20, Issue 7, pagg. 409-411.DOI: 10.1089/cyber.2017.0028/

Gli unici aspetti che parrebbero conformi ai tratti di personalità delle vittime tradizionali sono i tratti della coscienziosità e dell'apertura mentale: chi ha più autocontrollo - nello specifico, presta attenzione nell'aggiornamento dei programmi anti-malware ed evita d'avere un comportamento rischioso (es. scaricare contenuti da siti illeciti)[530]– e non è tanto curioso, è meno probabile che cada vittima di crimini cibernetici[531].

Vi è però una rilevante differenza rispetto alle vittime di reati tradizionali: a differenza di queste ultime, si è registrato che le vittime di reati cibernetici sono emotivamente più instabili[532].

Riguardo i tratti dell'estroversione e della gradevolezza, infine, non sono stati trovati collegamenti diretti con la vittimizzazione nel cybercrime[533].

Trattando adesso gli elementi che potrebbero far aumentare il rischio di vittimizzazione, è aspetto accolto in via unanime [534] che il quantitativo del tempo passato online sia direttamente proporzionale all'aumento della percentuale del rischio di restare vittima (di reato cibernetico e/o informatico che sia): a prescindere dal fatto se i propri *device* siano o meno protetti da appositi programmi, secondo la teoria delle attività routinarie stando molto tempo su Internet statisticamente ci si <<esporrebbe>> molto più frequentemente e a lungo nei "luoghi" in cui potrebbero trovarsi i potenziali offensori.

In particolare, si fa riferimento a:
a)La tendenza a fare <<click>> più velocemente sui link: questo è un chiaro segnale di un carattere propenso al rischio[535], che- come si è visto sopra - rende il soggetto più esposto alla vittimizzazione;
b) La condivisione di contenuto personale sui social media[536]: maggiore è il contenuto postato sui social, maggiore è la possibilità che il soggetto sia possa diventare vittima (es.

[530]Göttker, *op. cit.,* pag.15.
[531]Van de Weijer, Leukfeldt, *op. cit.,* pag. 409.
[532]*Ivi,* pag.408.
[533]Göttker, *op. cit.,* pagg.15-16. Si menziona però a pag. 16, che sono stati dimostrati scientificamente legami tra un comportamento rischioso nell'uso dei social media con l'estroversione e l'uso di un corretto comportamento di sicurezza online con la gradevolezza.
[534]Citando alcuni esempi: Virtanen, *op. cit*., pag.326.
[535]Junger, Hartel, Heydari, *op. cit*., pag. 5. Nello stesso senso: De Vivo, Ricci, *op. cit*.,pag. 58.
[536]Su questo punto vi sono ancora pareri discordanti: vi sono alcuni studiosi che, sulla base dei loro esperimenti, rilevano un effettivo nesso causale tra l'esposizione ai social media e l'elevatezza del rischio di divenire vittima, altri invece non individuano alcun nesso rilevante. Traiprimi:Choi,*Computer crime*

molestie online[537]), sia esporre soggetti terzi al rischio di vittimizzazione (es. l'azienda per cui il soggetto lavora[538]).

Importante segnalare che si fa riferimento al contenuto postato dalle vittime sia in via permanente che in via temporanea: in questo senso, si accenna al recentissimo utilizzo delle piattaforme dell'AI (l'Intelligenza Artificiale) creata da Google[539]come strumento per la realizzazione di nuovi reati[540].

c) L'acquisto o vendita online di beni: si è provato che più risulta esser il tempo speso in shopping online, maggiore risulta essere l'esposizione al rischio di diventare vittima di frodi bancarie e di truffe online. Inoltre, chiunque risulti eseguire un'attività avente ad oggetto la vendita di beni online, è allo stesso modo esposto anche alle frodi online da parte di <<falsi>> acquirenti, i quali frequentemente utilizzano carte di credito clonate[541].

d) L'intrattenimento online: il giocare a videogames ovvero guardare programmi televisivi, film, serie TV o contenuti pornografici in rete - specie se su siti illegali - rende inevitabilmente il soggetto più vulnerabile a possibili frodi online[542], nonché anche ad attacchi informatici di malware, in grado di ostacolare ovvero impedire il funzionamento del sistema informatico e telematico.

---

victimization and integrated theory: An empirical assessment, in *International Journal of Cyber Criminology*, 2008 Vol.2, pagg. 308–333. *Contra:*Junger, Hartel, Heydari, op.cit., pag. 5.

[537] Junger, Hartel, Heydari, *op. cit*., pag. 3, fanno in particolareriferimento a: Wilsem, *Hacking and harassment—do they have something in common? Comparing risk factors for online victimization*, in*Journal of Contemporary Criminal Justice*, 2013, Vol. 29, Issue 4, https://doi.org/10.1177/1043986213507402.

[538]Mazzarolo, Fernández Casas, Jurcut, Le-Khac in *ProtectAgainstUnintentional Insider Threats: The Risk of an Employee's Cyber Misconduct on a Social Media Site*, in *Cybercrime in context: the human factor*, a pag. 90 evidenziano come la propensione a dare informazioni personali della propria vita comporti la possibilità di fornire direttamente sui social informazioni sensibili relative all'azienda presso cui si lavora (o si ha lavorato)- o perlomeno, di fornire tracce da cui poter ricavare le informazioni (es. il ruolo che si occupa, l'articolazione della forza-lavoro in azienda, i turni di lavoro, ecc.).

[539]Per maggiori informazioni, si fa riferimento a : https://ai.google/ .

[540] Si fa riferimento sia all'utilizzo delle piattaforme dell'AI nel produrre qualsiasi voce (anche tramite contenuti postati temporaneamente nei profili social) allo scopo di commettere estorsioni e truffe; nonché al prendere delle foto (specie di celebrità) postate in rete ed <<incollare>> i volti su altri corpi a scopo pornografico. Citandoqualcheesempio: Verma, *Their voices are their livelihood. Now AI could take it away,* The Washington Post.com (24/04/2023), https://www.washingtonpost.com/technology/interactive/2023/ai-voice-generators/; Cost, *AI clones teen girl's voice in $1M kidnapping scam: "Ive got your daughter",* The New York Post.com (12/04/2023), https://nypost.com/2023/04/12/ai-clones-teen-girls-voice-in-1m-kidnapping-scam/; Tenbarge, *Found through Google, bought with Visa and Mastercard: Inside the deepfake porn economy*, Nbc News.com (26/03/2023) (https://www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071).

[541]Reep- van der Bergh, Junger, *op. cit*., a pag. 2; Van Wilsem, '*Bought it, but never got it'. Assessing risk factors for online consumer fraud victimization,* in*European Sociological Review*, 2013, vol. 29, Issue 2, pagg. 168–178 (DOI: https://doi.org/10.1093/esr/jcr053/).

[542]Junger, Hartel, Heydari, *op. cit*., pag. 5. Questo atteggiamento dell'utente viene appunto definito come <<comportamento rischioso online>> (<<rischy online behaviour>>) , ed è un fattore d'incremento del rischio di vittimizzazione online. V. pureGöttker, *The big five personality structure as a predictor for victimization in the context of cyber-crime*, University of Twente, 2021, pag.4.

Oltre al tempo trascorso online, altri aspetti che possono incidere sull'esposizione della potenziale vittima ai reati cibernetici ed informatici sono l'età e la conoscenza della tecnologia informatica. Riguardo la prima, nonostante statisticamente[543] la maggioranza delle vittime globali siano nella fascia tra i 30 e i 40 anni (seguiti subito dopo dalle persone d'età più anziana), più il soggetto è giovane, più è propenso a diventare vittima di reati cibernetici.

È stato poi accertato come una persona che non conosce bene la materia e non possiede abilità collegate alla tecnologia sia molto più propensa a cadere in contraffazioni e frodi online rispetto ad un esperto[544] - ragione per cui la persona più <<inesperta>> risulterebbe anche avere livelli più elevati di paura di cadere vittima di cybercrime[545].

In questa sede, si è voluto tentare di tracciare quelli che sono i profili generali della vittima di cybercrime: al fine di osservare meglio chi sarebbe potenzialmente più esposto a determinate tipologie di reati cibernetici e/o informatici rispetto ad altri, conviene chiudere la disamina del profilo della vittima eseguendo una classificazione delle diverse tipologie di cybercrime, guardando come criterio la tipologia d'interesse giuridico che viene minacciato.

La prima da tenere in considerazione è quella de i c.d. crimini cibernetici contro la proprietà. In essi rientrano tutte le tipologie di reato aventi come oggetto i dati bancari e /o le carte di credito di una persona (fisica o giuridica), l'accesso al commercio elettronico, le banche dati relative al sistema bancario[546]. Sono le forme più frequenti di cybercrime,

[543]Si fa riferimento a : https://surfshark.com/research/data-breach-impact/statistics/ .
[544]Göttker, *op. cit.,* pag.4. Nello stesso senso: Tonellotto, *op. cit.,* pag. 13.
[545]Virtanen, *op. cit.,* pag. 331.
[546]De Vivo, Ricci, *op. cit.,* pag. 56. Le Autrici,a pag. 57, parlano addirittura di <<monetica>>, ossia un nuovo settore che comprende tutte le truffe monetarie tramite l'uso di sistemi informatici; nonché anche dell'esistenza di un vero e proprio <<mercato>>mondiale di conti bancari on-line dove si importano e si rivendono ad altri le informazioni ed i codici stessi.

secondo le statistiche attuali[547], e vedono come vittime preferenziali le persone di età più anziana[548], nonché le aziende e le imprese[549].

La seconda categoria sono i c.d. crimini <<contro l'individuo>>: questi crimini hanno ad oggetto l'acquisizione, manipolazione e la diffusione di informazioni personali in rete. Aspetto comune risultano essere anche i danni psicologici ed emotivi che si portano dietro le vittime dopo aver subito la condotta criminosa[550]. In questa categoria rientrano il <<cyberstalking>>, il c.d. <<revengeporn>>, il <<cyberbullismo>>, nonchè le possibili tipologie di reati contro la libertà individuale e l'onore che possono verificarsi anche online (es. diffamazione o minacce tramite mail, video o messaggi[551]). Vittime preferenziali di questa categoria risultano essere le persone appartenenti alla categoria dei soggetti c.d.vulnerabili, in particolare: i bambini e gli adolescenti[552], le donne[553]; nonché le minoranze etniche[554], religiose, e gli appartenenti alla comunità LGBTQIA+[555].

Ultima categoria da tenere in considerazione (ma di non minore rilevanza) è quella del cybercrime<<contro il governo>>: in quest'ultima sono ricomprese le tipologie di reato

---

[547] Secondo una statistica globale del 2022 nel sito Statista.com (https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-global/), la forma più comune di reato cibernetico sarebbe quella del c.d. <<phishing>>, di cui è bastevole dire (per adesso) che si tratta di un reato cibernetico con finalità fraudolente. Seguendo la classifica, le forme di cybercrime più comuni sarebbero, nell'ordine: il furto d'identità online, la truffa del <<mancato pagamento/consegna>>, l'estorsione online, la truffa dei <<finti help-desk>>. Interessante dunque vedere che tutti questi reati appartengano a questa prima categoria, compreso il furto di identità, spesso usato per commettere frodi a nome altrui (De Vivo, Ricci, *op. cit.,* pag. 55-56).

[548] Per maggioriapprofondimenti, si fa riferimento a: Burton, Cooper, Dar, Matthews, Tripathi, *Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review,*in Experimental Gerontology, 2022, vol. 159;

[549] Per maggiori approfondimenti, si fa riferimento a: Wiggins, *Corporate Computer Crime: Collaborative Power in Numbers,* in*Federal Probation* , 2002, Vol. 66, Issue 3, pagg. 19-29.

[550] Kharat, *Cybercrime - A threat to persons,property, goverment and societies*, 2017, reperibile in: http://dx.doi.org/10.2139/ssrn.2913438/, pag. 5. Nellostessosenso: Henson, Reyns, Fisher *Cybercrime Victimization*, in Cuevas, Rennison, *The Wiley Handbook on the Psychology of Violence*, (a cura di); Wiley Blackwell, 2016, pag. 556.

[551]Kharat*, op. cit*., pag. 5

[552] Si cita sul punto: Fiocca, *Il darkside del cosmo digitale:"bersaglio- giovani". Le tutele*, in *Ciberspazio e diritto*, vol.20, n. 63(3-2019), pagg. 475-494; Van der Hof, Koops, *Adolescents and Cybercrime: Navigating between Freedom and Control*, in *Policy & Internet*, 2011, Vol. 3, Issue 2, Article 4. DOI: 10.2202/1944-2866.1121/ .

[553]Si fa riferimento a: Gurumurthy, Menon, *Violence against Women via Cyberspace*, in *Economic and Political Weekly* , 2009, Vol. 44, n. 40 (October 3-9, 2009), pagg. 19-21.

[554]Per maggioriapprofondimenti, si fa richiamo a:Gibbs, Hall;*Digital Ethnography in Cybercrime Research: Some Notes from the Virtual Field*, inLavorgna, Holt , *Researching Cybercrimes.Methodologies, Ethics, and Critical Approaches,* Palgrave Macmillan Cham; 2021;pagg.283-299 (https://doi.org/10.1007/978-3-030-74837-1/).

[555] Per maggiori approfondimenti,v.Meechan-Rogers, Bradbury Jones, Ward*; It's Just a Preference: Indigenous LGBTIQ+ Peoples and Technologically Facilitated Violence*, in Powell, Flynn, Sugiura, *The Palgrave Handbook of Gendered Violence and Technology*; MacMillian Cham, 2021, pagg.297-318.

meno frequenti, ma allo stesso tempo definite come le più pericolose[556]: si tratta di tutto quell'insieme di reati cibernetici - eseguiti da individui o da gruppi - minaccianti l'ordine pubblico degli Stati, tramite acquisizione di dati dai siti della pubblica amministrazione, del governo o delle forze militari, spesso a scopo politico, religioso, sociale ovvero propagandistico [557] . Alcuni esempi di reati rientranti nella categoria sono il cyberterrorismo[558] ed il cyberwarfare[559].

[556]Kharat*, op. cit*., pag. 7.
[557]*Ivi*, pag. 8.
[558]Per maggiori approfondimenti, si veda: Lamberti, *Gli strumenti di contrasto al terrorismo e al cyber-terrorismo nel contesto europeo,* in *Rivista di Criminologia, Vittimologia e Sicurezza*, 2014, Vol. VIII, n. 2 , pagg. 138-161.
[559]Secondo Kharat*, op. cit*., pag. 8., il cyber warfare consisterebbe nella attività di hacking posta in essere per motivi politici allo scopo di spionaggio e sabotaggio.

1.3.2. L'autore del reato cibernetico: profili criminologici.

Tanto variegato è il panorama delle vittime quanto lo è quello degli autori di reato nello spazio cibernetico: considerate le diverse tipologie di offese realizzabili nel ciberspazio, altrettanto diversi sono i panorami socio-ideologici in cui si collocano gli autori di reato, nonché le motivazioni in base a cui vengono commessi i reati e gli obiettivi che s'intendono raggiungere.

Bisogna però premettere che non si può fare una distinzione solo tra cybercriminali e i criminali <<tradizionali>>: infatti, gli autori di reato possono essere non solo esclusivamente operanti nel ciberspazio, ma anche operare alternativamente nella realtà fisica e in quella virtuale - ragione per cui gli studiosi premettono subito se l'oggetto del loro studio è rivolto agli autori di crimini informatici in senso stretto, ovvero in senso lato[560]. A ciò deve aggiungersi anche che essi possono agire singolarmente ovvero in gruppo (anche alternativamente), come pure l'emersione di diverse caratteristiche personali degli autori di reato in base alla tipologia di reati commessi; si rende dunque evidente la difficoltà che hanno gli studiosi[561] nel classificare con accuratezza e comparare i *profiling* dei cybercriminali con gli autori dei reati tradizionali.

Detto questo, si tenterà anche qui di dare uno sguardo generale agli autori di reato, vedendo nell'ordine quali possono essere le loro caratteristiche, la loro personalità e le motivazioni dietro la commissione dei loro reati, ed infine cercando di addivenire ad<<una tipizzazione degli autori coinvolti>>[562].

---

[560]V., ad esempio,Kranenbarg, Ruiter, van Gelder, Bernasco, *Cyber-Offending and Traditional Offending over the Life-Course: an Empirical Comparison,* in *Journal of Developmental and Life-Course Criminology*, 2018, Vol. 4, Issue 3, pag. 344. (DOI: 10.1007/s40865-018-0087-8/).
Si veda anche la ricerca di: Leukfeldt, Kolt, *Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals,* in *Computers in Human Behaviour*, 2022, Vol.126. (DOI: https://doi.org/10.1016/j.chb.2021.106979/), da cui si desume, a pag 7, in base alle interviste eseguite in Olanda, Regno Unito, Germania e negli USA, che quasi la metà degli autori di reato (48%) sembrerebbero specializzarsi in specifiche forme di reati cibernetici ovvero informatici, mentre circa il 10,8% degli offensori ha ammesso di commettere reati sia online che offline; identificando dunque una <<equità nella specializzazione come nella versatilità>>.
[561]Kranenbarg, *The challenges of Empirically Comparing Cybercriminals and Traditional Offenders,* in Lavorgna, Holt, *Researching Cybercrimes.Methodologies, Ethics, and Critical Approaches*; Palgrave Macmillan Cham, 2021, pag. 24(DOI: https://doi.org/10.1007/978-3-030-74837-1/).
[562]Tonellotto, *op. cit.,* pag.13.

Si dice, in linea di massima, che gli autori di reati cibernetici sono tendenzialmente maschi, giovani,[563] ed aventi un tendenziale disprezzo per la legge ovvero la sensazione di sentirsi superiori o inferiori alla legge stessa[564].

Queste informazioni però danno vita ad un panorama piuttosto esiguo della figura dell'autore di reati cibernetici e/o informatici: sarà dunque necessario iniziare dall'elencazione dei tratti socio-economici che si presentano più frequentemente in questi soggetti. In particolare:

- A differenza dell'autore di reati tradizionali, vi è la tendenza a ritenere che l'autore solo di reati cibernetici sia di uno status socioeconomico superiore rispetto alle proprie vittime[565],

- Un fattore in discussione è la conoscenza tecnologica: spesso l'autore di questi reati ha acquisito competenze nel sistema informatico e ha conoscenze maggiori su quel campo rispetto ad una persona media[566];inoltre numerosi studi dimostrano che un tratto ricorrente è l'alto livello formativo dell'individuo[567].
  Tuttavia, questo non è necessariamente un dato perentorio, sia per il fatto che autore del reato (seppur raramente) può essere anche colui che commette un reato cibernetico per la poca familiarità con la tecnologia; ma anche perché vi sono stati studi da cui risultava che i cybercriminali tendevano ad interrompere gli studi superiori ovvero universitari[568]. In aggiunta,la conoscenza nel campo informatico non comporta automaticamente che il soggetto sia anche più intelligente rispetto alla media:è stato provato scientificamente che, seppur molti cybercriminali abbiano ottenuto un punteggio più alto nei test rispetto ai

[563]Donner, Marcum, Jennings,Higgins, Banfield, *Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy*, in *Computers in Human Behaviour*,2014, Vol.34, pag.166. (DOI: https://doi.org/10.1016/j.chb.2014.01.040/)
[564] Koops, Jaap, *The internet and its opportunities for cybercrime,* in: Herzog-Evans. *Transnational Criminology Manual,*Wolf Legal Publishers (WLP), 2010, pag. 739, fannoriferimento in particolarea :Shinder, Cross, *Scene of the Cybercrime, cit.,* 2008, Syngress ed., pagg. 88, 93-94 (DOI: https://doi.org/10.1016/B978-1-59749-276-8.00003-0/)
[565]Leukfeldt,*Research Agenda. The Human Factor in Cybercrime,*pag.23.
[566]Secondo: Kranenbarg, Ruiter, van Gelder, Bernasco, *op. cit.,* pag. 348, è dimostrato che la conoscenza dei sistemi informatici nonché l'acquisizione di competenze tecnologiche fa aumentare la possibilità che l'individuo commetta reati cibernetici- specie sul posto di lavoro, contro l'azienda stessa per cui lavora.
[567]Leukfeldt , *op.cit,* ,pag.25.
[568]Schiks, van de Weijer ,Leukfeldt, *op. cit*., pag. 2, fa riferimento a:Chan, Wang, *Profiling Cybercrime Perpetrators in China and its Policy Countermeasures*, cit., in Smith, Chak-Chung Cheung, Yiu-Chung Lau , *Cybercrime Risks and Responses*, Palgrave Macmillan,2015,.DOI: (https://doi.org/10.1057/9781137474162_14/), dove si riporta che spesso alcuni hacker tendano a mollare gli studi, perché <<troppo noiosi>> o <<fin troppo facili>>.

criminali di reati tradizionali, è comunque un punteggio inferiore rispetto alla media ottenuta dai non-criminali[569].

- Secondo alcune teorie criminologiche, una compagine sociale solida e sana renderebbe l'individuo più desideroso di conformarsi alla società, e quindi meno predisposto a commettere crimini[570]: ora, è stato provato che l'avere al proprio fianco una famiglia e/o una relazione amorosa farebbe decrescere nei cyber criminali l'interesse a commettere crimini in misura molto più elevata rispetto ai criminali tradizionali.
  Tuttavia – al pari del punto precedente - non si può desumere in linea assoluta che il cybercriminale sia necessariamente una persona isolata socialmente: non è preclusa la possibilità che l'attore commetta reati cibernetici anche in presenza di una componente sociale compresente nella sua vita; parrebbe che la presenza di un nucleo familiare con un genitore singolo faccia aumentare la probabilità di propensione alla commissione ai reati cibernetici molto di più rispetto a quelli tradizionali[571].

- Infine, bisogna dare uno sguardo all'aspetto lavorativo: dagli studi sembrerebbe esserci un forte legame tra l'occupazione e la diminuzione della propensione a divenire cybercriminali - sia per la paura di perdere il proprio lavoro se si commette un crimine, sia per l'attività di controllo che esercita il superiore sull'operato del dipendente[572]. Come però visto negli ultimi due punti precedenti, in realtà non sempre la disoccupazione è un elemento chiave per il profilo dell'autore di reati cibernetici: in primis, il computer è divenuto oggi parte della vita quotidiana e lavorativa (perciò, chi lavora in media ne farebbe un uso molto più elevato rispetto al soggetto disoccupato); ma è stato pure rilevato che lo specifico impiego nel settore informatico e tecnologico farebbe aumentare esponenzialmente la possibilità di commissione di reati cibernetici rispetto a quelli tradizionali[573].

---

[569]Schiks , van de Weijer, Leukfeldt,*High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals,* in Computers in Human Behaviour, Vol.26, 2022, pag. 5 (DOI:https://doi.org/10.1016/j.chb.2021.106985/).

[570]Kranenbarg, Ruiter, van Gelder, Bernasco, *op. cit.,*pag.345, fannoriferimento a: Morizot, Kazemian, *The development of criminal and antisocial behavior.Theory, Research and Practical Applications,* 2015, Springer (DOI: https://doi.org/10.1007/978-3-319-08720-7/) . In particolare, questo aspetto farebbe diminuire antisocialità dell'individuo - elemento della personalità che può decisamente influire nella sua scelta d'iniziare una carriera criminale, a prescindere se questo avvenga nella realtà fisica o virtuale (o in entrambe).

[571]*Ivi*,pagg. 355-356.

[572]*Ivi*, pag. 348.

[573]*Ivi,* pag. 345.

Se gli studi menzionati finora sulle caratteristiche comuni sono numerosi, di carattere recente e ancora con poche certezze, altrettanto lo sono i tentativi svolti sullo studio della personalità del cyber criminale.

Da quello che abbiamo visto riguardo il profilo della vittima sulla teoria dell'autocontrollo, anche il soggetto attivo del reato può esser impulsivo avere poco autocontrollo[574]: è necessario indicare però che - diversamente dalla persona offesa nel cyber criminale è coesistente, assieme all'impulsività, l'assoluta o parziale insensibilità di percepire come prevalente il peso del dolore arrecato agli altri rispetto al piacere personale conseguito dalle proprie azioni - forse dovuta proprio all'assenza di contatto fisico tra autore e vittima nella commissione del fatto tipico.[575]

Come si potrà intuire, trarre solo quest'aspetto sulla personalità dell'individuo è eccessivamente riduttivo. Perciò, per dare una visione più complessiva su questo tema, si guarderanno due diversi studi eseguiti sulla base di due diverse teorie psicologiche.

La prima risulta essere quella delle sei dimensioni della personalità (il c.d. modello <<HEXACO>>[576]), sviluppata sulla base della teoria dei c.d. <<Big Five>> già summenzionata. Sulla base di uno studio condotto in Olanda[577] in comparazione tra un gruppo di criminali sul piano cibernetico, un gruppo di criminali <<tradizionali>> ed uno di non-criminali, si sono potuti trovare dei risultati interessanti.

---

[574]Donner, Marcum, Jennings,Higgins, Banfield, *op.cit.,* pag. 171. Nellostessosenso:Holt, Bossler,May, *Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance*, in *American Journal of Criminal Justice,*2012, Vol.37, Is. 3, pag.380 (DOI:https://doi.org/10.1007/s12103-011-9117-3/). *Contra*:Leukfeldt, *Research Agenda. The Human Factor in Cybercrime and in Cybersecurity,*2017, Eleven International Publishing, pag.25; Kranenbarg, van Gelder, Barends, de Vries, *Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personalitydomains and theirunderlyingfacets,*in*Computers in Human Behaviour,*2023, Vol.140, (DOI: https://doi.org/10.1016/j.chb.2022.107576/), pag. 9, in cui- come si dirà nelle pagine seguenti- si dispone che i cyber criminali tendono ad esser molto più cauti e a non perdere la tempra facilmente.

[575]Donner,Marcum, Jennings,Higgins, Banfield, *op. cit.,* pag.166. Nello stessosenso: Kranenbarg, van Gelder, Barends, de Vries, *op. cit*., pag.9.

[576] Questateoria, posta per la prima voltada : Lee, Ashton, *Psychometric properties of the HEXACO personality inventory*, in *Multivariate Behavioral Research,*2004, Vol.39, Issue 2, pagg.329-358(DOI:https://doi.org/10.1207/s15327906mbr3902_8); ha il pregio di aggiungere, oltre ai tratti già summenzionati delle cinque dimensioni della personalità, un sesto elemento, il c.d. <<fattore H della personalità>>: tramite questo modello, si misura anche il tratto della Onestà-Umiltà. Le persone con punteggi alti su questo tratto evitano di manipolare gli altri per guadagno personale e non sono tentati dall' infrangere le regole. Al contrario, le persone con punteggi bassi tendono a lusingare gli altri per ottenere ciò che vogliono e sono inclini a infrangere le regole per profitto personale.

[577]Kranenbarg, van Gelder, Barends, de Vries, *op. cit.,* pagg.7 e ss.

In sostanza, da questi studi risulta che il cybercriminale è esaltato in tutti gli aspetti del tratto della Coscienziosità (Perfezionismo, Prudenza, Organizzazione, Diligenza [578]), nonché risulta avere un elevato livello nella Pazienza, sottogruppo del tratto della Gradevolezza: questo spiega le spiccate caratteristiche del soggetto nella disciplina, pazienza e le sue doti di calcolatore e la sua minor impulsività rispetto ad un criminale tradizionale.

Ma non è solo questo il dato da registrare: altro aspetto essenziale che emerge dai risultati è che i punteggi dell'autore di reati cibernetici riguardo i tratti di personalità dell'Onestà, del Nevroticismo e della Estroversione fossero molto più vicini a quelli del gruppo dei non-criminali rispetto a quelli degli autori di reati tradizionali (fatta eccezione per alcune differenze rilevanti per determinati sottogruppi, come: il basso livello sulla Modestia, sulla Flessibilità, nonché un elevato livello di atteggiamento evitante e Curiosità[579]).

La seconda teoria da riportare è invece la c.d. <<Teoria della Triade Oscura delle Personalità>>[580]: tre tratti della personalità (Narcisismo, Machiavellismo e Psicopatia[581]) che- a livelli più estremi- sono condivisi dai criminali o da chi soffre di gravi malattie

---

[578]Per darne una breve definizione: la scala dell'Organizzazione valuta la tendenza a cercare l'ordine, la Diligenza valuta la tendenza a lavorare sodo, nel Perfezionismo si valuta la tendenza ad essere accurati e attenti ai dettagli, infine nella scala della Prudenza si valuta la tendenza a controllare gli impulsi.
Vi sono due considerazioni interessanti da fare sul punto:

- *in primis*, con questi dati si conferma quanto detto prima sulla prevalenza del piacere personale rispetto al dolore arrecato agli altri in seguito alle proprie azioni;
- in base al livello basso di modestia emerge che l'autore di questi reati spesso si senta superiore agli altri anche perché rischia di esser individuato dalle autorità con meno frequenza rispetto ad un criminale tradizionale.

[579]Andando più nel dettaglio: la Modestia è una scala dell'Onestà, la Flessibilità è una sottoscala della Gradevolezza, infine la Curiosità è una sottoscala dell'Apertura Mentale.
Dai risultati ottenuti dagli Autori summenzionati nelle note precedenti, si desumerebbe che il cybercriminale, nell'ordine: ha un'alta opinione di sé, è motivato a perseguire il possesso di beni materiali, preferisce perseguire il proprio interesse personale piuttosto che trovare un punto d'incontro con altri, è disposto ad approfondire per ottenere ulteriori informazioni.

[580] Paulhus, Williams, *Thedark triad of personality: Narcissism, Machiavellianism, and psychopathy*, cit., in *Journal of Research in Personality*, 2004, Vol. 36 Issue 6, pagg. 556–563. (DOI: https://doi.org/10.1016/S0092-6566(02)00505-6/)

[581]Prendendo le definizioni fornite da: Selzer, Oelrich, *op.cit.,* nelle pagg.176-177:

- il Narcisismo è proprio di una persona che cerca ammirazione negli altri e manca di empatia. Tratti tipici di una persona narcisista sono il senso di grandiosità, l'incentrarsisu sé stessi e la sensazione di esser privilegiato (in base alla quale il soggetto sfrutta gli altri a proprio vantaggio);
- il Machiavellismo è proprio di una persona definita <<moralmente flessibile>>: chi possiede questo tratto della personalità è una persona fredda, che considera ed utilizza le persone più o meno come oggetti per il raggiungimento dei propri interessi personali.
- La Psicopatia corrisponde ad una cronica e pervasiva disposizione ad ignorare e violare le regole altrui. Le manifestazioni di questo tratto includono: aggressività, impulsività, ripetute violazioni della legge, mancata considerazione delle conseguenze per gli altri delle proprie azioni,accompagnata da assenza di senso di colpa o rimorso.

mentali. Dai risultati ottenuti sugli studi relativi a questa teoria sui cybercriminali[582], due di questi tratti- il Machiavellismo e la Psicopatia- parrebbero incentivare il soggetto alla commissione di reati nel ciberspazio, mentre il Narcisismo non sembrerebbe esser direttamente collegato alle motivazioni dei cybercriminali nel commettere reati.
In particolare, la Psicopatia è un tratto presente anche spesso negli autori di reati tradizionali: considerata la definizione di questo tratto, si dedurrebbe che i criminali tradizionali aventi alti livelli di Psicopatia potrebbero vedere il cyberspazio come terreno ulteriore per la commissione di reati – ragione per cui per loro sarebbe visto come conveniente <<digitalizzare la propria condotta criminale>>[583] ovvero eseguire attività criminali alternativamente su entrambi i fronti (digitale e virtuale).

Da queste due ricerche, si permette pertanto di cogliere la peculiarità della figura dell'autore dei reati cibernetici sul piano della personalità: da un lato,vi sono:la freddezza, la prudenza, la pazienza e la noncuranza per gli altri delle conseguenze proprie azioni che lo predispongono alla commissione di reati. Dall'altro lato, emerge il possesso di non pochi aspetti vicini ai parametri medi dei soggetti non-criminali – tratti che, secondo gli studiosi[584], sono tutt'altro da ignorare, perché sono quelle stesse caratteristiche che agevolano il soggetto alla commissione dei reati cibernetici.

Un ulteriore aspetto da tenere in considerazione è il perché queste tipologie di autori commettono reati nel cyberspazio.
Anche questo è un campo di ricerca recente ed in continua evoluzione: vi sono stati diversi studi in cui sono eseguite delle categorizzazioni sulle tipologie dei diversi criminali che operano nel cyberspazio in base alle loro competenze ed alle ragioni in base alle quali agiscono[585], ma vi sono state altrettante critiche su queste classificazioni, in quanto la maggioranza di esse prenderebbero in riferimento delle assunzioni generali o non sempre attendibili[586]. In ogni caso, anche qui si tenterà di fare un discorso generale, sulla base

[582]Selzer, Oelrich*, op. cit.,*pagg. 185-187.
[583]*Ivi,* pag.188.
[584]Kranenbarg, van Gelder, Barends, de Vries,*op. cit.,* pag.7.
[585]Un classico esempio lo si ritrova negli studi eseguiti sulla figura dell'hacker in: Seebruck,*A typology of hackers: Classifying cyber malfeasanceusing a weightedarccircumplex model,*in *Digital Investigation,*2015,Vol. 14, pagg. 36-45. (DOI:https://doi.org/10.1016/j.diin.2015.07.002.)
[586] Kranenbarg, *Cyber-Dependent Crime Versus Traditional Crime: Empirical Evidence for Clusters of Offenses and Related Motive,* in AA.VV., *Cybercrime in context: the Human factor,* a pag.197, fa in particolare riferimento a: Morris, *Computer hacking and the techniques of neutralization: An empirical assessment*, in: Holt, Schell, *Corporate hacking and technology-driven crime: Social dynamics and implications,*, New York, NY: Information Science Reference, 2011, pag.1–17.

degli studi scientifici svolti in comparazione tra gli autori di reati tradizionali e gli autori di reati informatici in senso stretto. [587]

Viene indicato che – in linea di massima[588] - la commissione di reati informatici/cibernetici in senso stretto spesso avviene per una motivazione intrinseca (la commissione del reato in sé) piuttosto che per motivazioni estrinseche (<<le conseguenze esterne susseguenti alla commissione della condotta illecita>>[589]; es. soldi, ottenere vendetta, ecc.). Tuttavia, tenendo conto che sono state individuate numerose condotte mosse da fattori che farebbero fatica a rientrare nella categoria delle motivazioni intrinseche (es. idee di carattere politico/religioso), è bene soffermarsi meglio su quelle che possono essere le ragioni più frequenti, ossia le diverse tipologie di motivazioni - intrinseche ed estrinseche – che spingono i soggetti a commettere reati informatici in senso stretto.

In base ai risultati ottenuti dalle ricerche, risulterebbe che:

a) è confermato che i motivi intrinseci sono i più frequenti: motivazioni da segnalare sul punto sono: la <<noia/curiosità/semplice divertimento>>, nonché la <<sfida/stimolo intellettuale>>, poiché non si trovano nei reati dei c.d. <<colletti bianchi>> e nei reati tradizionali con la medesima frequenza[590].
b) Le ragioni finanziarie sono spesso più assenti per questa categoria di reati(questo però non esclude che non siano presenti per i reati informatici in senso lato[591]);
c) i motivi estrinseci in realtà (es. <<per rabbia/vendetta/bullizzare qualcuno>>, <<metter le cose in chiaro/inviare un messaggio>>, <<ottenere il rispetto degli altri/potere>>[592]) sarebbero invece più presenti per i reati informatici in senso lato che in quelli in senso stretto.

Infine, a chiusura di questa disamina, è interessante segnalare anche un'ulteriore ragione di carattere sociale: purtroppo il mondo del crimine cibernetico viene spesso visto come l'unica strada per giovani talenti in matematica ed informatica che nei paesi aventi

[587]Si fa riferimento a: Kranenbarg, *op. cit*., in *Id*., Leukfeldt, *Cybercrime in context: The human factor,* cit..
[588] Steinmetz, *CRAFT(Y)NESS: An Ethnographic Study of Hacking*, in *The British Journal of Criminology,* 2015, vol.55, Issue 1, pagg. 125–145. (http://www.jstor.org/stable/43819263/)
[589]Kranenbarg, *op. cit*., pag. 197.
[590]*Ivi,* pag. 207.
[591]Oltre al fatto che (come individuato prima nei profili delle vittime) le forme più frequenti di reati online sono le truffe online (i c.d. *scam),* ma anche è presente la diffusione dei <<crimini dei colletti bianchi>> (commessi da una persona rispettabile nel corso della propria occupazione) anche online, compiuta sia da offensori di carattere esterno- individui che accedono ai sistemi per agire online contro aziende ed imprese, sia di carattere interno- individui che agiscono contro la stessa impresa per cui lavorano. Inutile dire che entrambi i casi gli autori di reato agiscono per motivi finanziari.
Per maggiori approfondimenti sull'argomento: Gottschalk,Hamerton, *White-Collar Crime Online: Deviance, OrganizationalBehaviour and Risk*, 2022, PalgraveMacmillan. (DOI: https://doi.org/10.1007/978-3-030-82132-6_4/)
[592]Kranenbarg, *op. cit*., pag. 205.

un'economia in via di sviluppo non riescono a trovare un lavoro nel settore IT ovvero che non ottengono abbastanza denaro dai loro lavori[593].

In chiusura alla disamina della figura dell'autore di reato, si guarderà alle principali tipologie di autori di reato nei sistemi informatico e cibernetico improntate al raggiungimento di interessi economici e/o per motivazioni di carattere ideologico(in particolare, coloro che sono in grado di minacciare la c.d. <<cybersecurity[594]>>).Più specificamente, si vanno a considerare cinque diverse categorie di agenti:

i. Il <<petty criminal>>[595] (letteralmente, il <<criminale di minore importanza>>): si tratta di piccoli gruppi o soggetti singoli che, tramite un apposito sistema di e-mail, invogliano gli utenti a fornire loro dei propri dati sensibili, in modo da poter violare ed accedere ai loro sistemi. Nonostante questo, sono tuttavia noti anche per la rapidità nel cambiamento della loro vittima se riscontrano che essa abbia attivato un minimo livello di sicurezza per i propri sistemi informatici e telematici. Questi ultimi non possiedono particolari abilità informatiche rispetto alle altre categorie di criminali che si elencheranno in seguito, ma possono essere utenti esterni tanto quanto soggetti interni allo stesso ente colpito.

ii. Le <<cyber gang>>: si tratta di gruppi criminali aventi lo scopo di arricchirsi illecitamente. Spesso utilizzano diversi strumenti informatici (ad es. tramite il *phising* o l'uso dei *malware*[596]) in modo da acquisire informazioni da usare con finalità estorsive[597], ovvero <<per […] gestire in maniera fraudolenta i sistemi di pagamento delle singole vittime>>[598].

iii. I c.d. <<competitor>> o i <<National state-sponsored>>, gruppi che hanno l'obiettivo di acquisire informazioni strategiche in modo da ottenere un vantaggio enorme sul piano

[593]Kshetri, *Diffusion and Effects of Cyber-Crime in Developing Economies*, in *Third World Quarterly* , 2010, Vol. 31, n. 7, pag.1071. (https://www.jstor.org/stable/27896600/)
[594]Fowler, *Cybersecurity*, in: Green, *Enterprise Risk Management. A Common Framework for the Entire Organization*, 2016, Butterworth-Heinemann (DOI:https://doi.org/10.1016/C2013-0-18651-5/) a pag.91 definisce la cyber security come <<l'insieme delle tecnologie,processi e attività necessarie per proteggere i network, computer, dati ed i sistemi da un attacco, un danneggiamento o un accesso non autorizzato>>.
[595]Fowler, *op. cit*., pag.94.
[596]Secondo la definizione data da: Pascuzzi*, op. cit*., pag.372, il malware è un <<software dannoso progettato specificamente per danneggiare o interrompere un sistema, attaccando la riservatezza, l'integrità o la disponibilità>>.
[597]Come indicato da: Tonellotto, *op. cit.,* pag. 14, molto spesso utilizzano una specifica tipologia di <<phishing distribuito>> (c.d. *spear phishing*), nonché di software in grado di danneggiare o rendere inservibili i sistemi colpiti, in modo da chiedere successivamente un riscatto alla vittima per permetterne il ripristino.
[598]Tonellotto, *op. cit.,*pag. 14.

economico, industriale, commerciale, politico o militare[599]- spesso su commissione diretta anche delle istituzioni nazionali per coadiuvare ovvero eseguire direttamente attacchi cibernetici [600].

A differenza delle cyber gang, questi gruppi possiedono molta più competenza e capacità tecnica: in particolare, utilizzano la tecnica dell'APT (<<*Advanced Persistent Threat*>>), allo scopo di infiltrarsi nel sistema-bersaglio per << acquisire informazioni riservate, […] prendere il controllo dell'infrastruttura attaccata>>[601], nonché distruggere le informazioni stesse. Queste tipologie di attacchi si caratterizzano sia per la loro sofisticata complessità, ma anche per la loro capacità di permanere per lungo tempo all'interno del sistema attaccato.

Questi gruppi recentemente si caratterizzano anche per l'attività di disinformazione, allo scopo di disseminare in rete <<notizie non veritiere, del tutto false o forvianti nei confronti di avversari politici>>[602].

iv. Gli *scammer*: soggetti che hanno l'obiettivo di rubare informazioni personali ovvero denaro agli utenti in via fraudolenta per poi sparire nel nulla, e che si caratterizzano per la forte abilità di persuasione. Le tipologie di truffe online sono diverse e numerosissime, ma si può fare un cenno a due gruppi. Un primo gruppo corrisponde ai c.d. <<scam finanziari>>: truffe aventi ad oggetto la possibilità di dar vita a delle attività economiche fasulle illudendo i soggetti della enorme possibilità di guadagno. Altra tipologia degna di menzione e il c.d. <<scam sentimentale>>: in quel caso lo *scammer* ha previamente acquisito informazioni personali sulla vittima, e, tramite chat, e-mail o social network, tenterà di sfruttare lo stato emotivo della vittima chiedendogli denaro (es. aiuto economico per situazioni gravi o tragiche).

v. Postutto, bisogna considerare una figura particolare, ossia quella degli <<hacktivisti>>, soggetti spinti da motivazioni politiche ed ideologiche ad eseguire attacchi informatici contro aziende industriali, ma anche istituzioni ed organizzazioni che sono contrarie alla

[599]Friedman, Bouchard, *Defintive Guide to Cyber Threat Intelligence*,Cyber Edge Press, 2015, pag. 14.

[600]Come indicato da Fowler, *op. cit*., pag.96; un esempio è il caso del c.d. Elderwood Group, un gruppo che ha recentemente eseguito più di 300 attacchi cibernetici contro il sistema militare statunitense, nonché governi e grandi aziende tecnologiche.

[601]Tonellotto, *op. cit.,* pag. 15.

[602] Si fa in particolare riferimento al Report del Threat Analysis Group di Google nel 2019 (https://blog.google/threat-analysis-group/), in cui si sono riportati i tentativi di hacking commissionati da governi non occidentali: emerge che vi sono stati oltre 270 gruppi aventi legami con i governi di più di 50 paesi, specializzati nella raccolta di informazioni, nel furto di proprietà intellettuali ovvero in attacchi informatici ai danni di dissidenti politici, giornalisti e attivisti scomodi, nonché nell'attività di disinformazione nei loro confronti.

loro visione[603] - spesso questi attacchi consistono nella divulgazione di dati sensibili screditanti la vittima, ovvero in Denial of Service (<<DoS>>), attacchi volti a bloccare temporaneamente il sistema informatico o cibernetico[604].
L'hacktivista può agire da solo, ma - come ben si vedrà nella parte dedicata alle associazioni a delinquere online - nella maggioranza dei casi fa parte di gruppi organizzati e composti da altri numerosi utenti che condividono le stesse ideologie ovvero obiettivi.

Non si andrà oltre in questo paragrafo sulla trattazione di questi ultimi e neanche sul loro più famoso esempio, l'Organizzazione Anonymous: è bastevole per il momento menzionare il fatto che è spesso sorge il dubbio nell'opinione pubblica se questi soggetti debbano essere effettivamente considerati autori di reato - a maggior ragione se agiscono per <<una causa>> moralmente condivisa[605].
Questo però non fa venire meno la loro pericolosità, considerando che le loro abilità tecnologiche possono dar vita a gravi conseguenze politiche, economiche e sociali - o meglio, ad <<una condotta multi - offensiva con risvolti *high-tech*>>[606].

[603]Fowler, *op. cit*., pag.95.
[604]Di questi ultimi si fa un diretto rinvio al Capitolo III.
[605] George, Leidner, *From clicktivism to hacktivism: Understanding digital activism*, in *Information and Organization,* 2009, Volume 29, Issue 3, pag. 15. (DOI: https://doi.org/10.1016/j.infoandorg.2019.04.001/).
[606]Tonellotto, *op. cit*., pag. 16.

2.Il contrasto transnazionale alla crescita del fenomeno Cybercrime.

Questa nuova dimensione cibernetica della criminalità ha portato non poco fermento nel sistema giuridico, tanto che i principali cambiamenti arrecati al sistema cibernetico con l'apertura di Internet all'intera popolazione globale si son tradotti nei termini: *Destatualizzazione, Deterritorializzazione, Dematerializzazione*[607].

Definiti i tratti generali del *cybercrime*, non si può disquisire sul tema ignorando questi aspetti[608], partendo in primo luogo dal primo di essi. Considerata la c.d. <<aterritorialità della Rete>> accennata nel paragrafo precedente, si comprese bene come il sistema informatico e cibernetico non solo aveva messo in crisi il concetto di sovranità dello Stato[609] (in particolare il fatto che <<lo Stato sia il soggetto principale (se non esclusivo) abilitato a porre le regole>>[610]), ma aveva fatto capire presto ai singoli Stati che la dimensione delle attività in Rete- reati compresi- aveva raggiunto un'estensione talmente ampia che non poteva non essere non trattata se non in via sovranazionale.

Ecco perché non si può parlare del *cybercrime* senza enunciare le principali risposte a livello internazionale ed europeo, e senza chiedersi se esse siano bastevoli per contrastare efficacemente questo fenomeno: i tempi di mutamento del sistema cibernetico ed informatico sono molto più repentini e numerosi rispetto alla lentezza della formazione di una sentenza definitiva all'esito di un processo - men che meno per il tempo necessario per la formazione ed emanazione della normativa. È importante dunque richiamare l'attenzione sulla presenza d'un costante <<affanno>> della dottrina e della giurisprudenza (nazionale e sovranazionale) nel porre norme efficaci e puntuali rispetto ad un sistema con caratteristiche radicalmente diverse e con ritmi molto più veloci rispetto alla realtà fisica.

Ultima considerazione da fare è che gli atti e gli strumenti normativi che saranno analizzati nel prosieguo della trattazione si sono ampiamente occupati anche della dimensione

---

[607]Si fa riferimento a : Pascuzzi, *op. cit.,* pagg. 353 e ss.

[608]L'aspetto della *Deterritolizzazione* verrà ripreso nel punto 3.2; mentre la *Dematerializzazione* non verrà particolarmente approfondita, considerata la tematica trattata in questa sede. È sufficiente dire che essa consiste sia nella ridefinizione dei beni giuridici (il dato informatico, le banche dati, ecc.), sia negli effetti dell'era digitale sugli atti ed i fatti giuridici (es. il documento digitale, la sottoscrizione digitale, ecc.), come si rileva in: Pascuzzi,*op. cit.,* pagg. 361-363.

[609]*Ibidem.*. Nello stesso senso:Mattarella, *La futura Convenzione ONU sul Cybercrime e il contrasto a nuove forme di criminalità informatica*, in Sistema Penale, 2022, Vol.3 , pag. 43. (https://www.sistemapenale.it/it/fascicoli/fascicolo-mensile-2022-3/)

[610]*Ibidem.*

processuale – sottoponendo perciò quellasovranazionale ed italiana ad importanti revisioni - ma, considerata la tematica dell'elaborato in questione, si guarderà solo ai profili penali sostanziali.

2.1.La dimensione internazionale: la Convenzione Cybercrime del 2001.

Bisogna dunque partire dalla Convenzione Cybercrime approvata a Budapest il 23 novembre 2001 (definita dunque anche come <<Convenzione di Budapest>>) dal Consiglio d'Europa.

Non a caso viene considerata il più importante strumento contro la criminalità informatica a livello globale: rispetto agli atti adottati negli anni precedenti[611], questa Convenzione ha l'obiettivo di rafforzare il diritto penale e processuale penale, e migliorare la cooperazione giudiziaria e di polizia al fine di contrastare più efficacementesia <<la criminalità […] "cibernetica"- nelle sue nuove forme e caratteristiche globali, ma anche quella "comune" che utilizzi come mezzo la rete >>[612].

Ma non solo: punto di forza della Convenzione è anche il fatto che da essa non traspare l'obbligo per gli Stati aderenti di mera trasposizione delle norme contenute in essa, quanto piuttosto dei valori in essa tutelati. Tra essi, emerge una peculiare <<valutazione politico-criminale sull'uso di nuove tecnologie>>[613], la quale è dovere degli Stati effettuare ed adattare al loro sistema (sempre considerando il margine di discrezionalità che hanno a disposizione).

Quest'ultimo aspetto si riesce appunto a percepire già nella Sezione I della Convenzione, dove si prevede che ogni Stato aderente alla Convenzione deve predisporre le misure

[611]Fino a quel momento infatti erano state poste in essere Raccomandazioni, rivolte ad una cerchia ben più ristretta di Stati destinatari e relative ad ambiti più settoriali. Dalla scelta di dar vita ad una Convenzione e non ad una Raccomandazione - potendo in questo modo ampliare le tematiche da trattare- e da quella di dare la possibilità di aderire anche a Stati <<terzi>>, estranei al Consiglio d'Europa, si desume la percepita urgenza di un mezzo idoneo a contrastare un fenomeno globale, consentendo allo stesso tempo il massimo livello di armonizzazione dei sistemi legislativi e processuali dei vari Stati aderenti. Per maggiori approfondimenti sul punto, si cita: García, *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul Cybercrime*, in Picotti, *Il diritto penale dell'informatica nell'epoca di Internet*, 2005, CEDAM, pagg. 129-131; Flor, *Cyber-criminality: le fonti internazionali ed europee,* in: Cadoppi, Canestrari, Manna, Papa, *Cybercrime*, UTET Giuridica, 2019, pagg. 104 e ss.

[612]Picotti, *Sistematica dei reati informatici,* pag. 29.

[613]García, *op. cit.*, pag. 124.

legislative necessarie affinché vengano configurati come reati nella propria legge nazionale le seguenti fattispecie, che possono esser ricomprese in quattro macroaree:

a) I reati contro la riservatezza, l'integrità e la disponibilità dei dati [614] e dei sistemi informatici [615]. Si tratta delle seguenti fattispecie: l'accesso illegale ad un sistema informatico (art.2)[616], l'intercettazione abusiva (art.3)[617], l'attentato all'integrità dei dati (art.4)[618], attentato all'integrità del sistema (art.5)[619], l'abuso di apparecchiature (art.6)[620];
b) I <<reati cyber-correlati>>[621]: in esso vengono ricompresi quei reati tradizionali che possono esser commessi tramite le TIC, ossia: la falsificazione informatica (art. 7)[622] e la frode informatica (art.8)[623];

---

[614]Secondo l'art. 1, lett. b) della Convenzione di Budapest,per <<dati informatici>> si intende: <<qualunque rappresentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione>>.

[615] Secondo l'art.1, lett. b), della Convenzione, per <<sistema informatico>> s'intende <<qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati>>.

[616]In base all'art.2, comma 1, della Convenzione: la condotta oggetto di un obbligo di penalizzazione da parte degli Stati consiste nell'<<accesso all'intero sistema informatico o a parte di esso senza autorizzazione.>> Al comma 2 si dà la possibilità agli Stati di richiedere che il reato venga commesso con lo specifico <<intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico>>ovvero mediante la violazione di <<misure di sicurezza con l'intenzione di ottenere informazioni all'interno di un computer>>.

[617]In base all'art.3[1] della Convenzione s'intende:<<l'intercettazione senza autorizzazione, fatta con strumenti tecnici, di trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema informatico, incluse le emissioni elettromagnetiche da un sistema informatico che ha tali dati informatici>>. Come nella nota precedente, s'include la possibilità di prevedere la commissione del reato tramite lo specifico <<intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico>>.

[618]In base all'art.4, comma 1, della Convenzione, si fa riferimento al <<danneggiamento, la cancellazione, il deterioramento, la modifica o la soppressione di dati informatici senza autorizzazione>>. Al comma 2 si aggiunge che è possibile, per gli Stati, prevedere che l'entità del reato sia di <<grave danno>>.

[619]In base all'art.5, comma 1, della Convenzione, si fa riferimento al <<serio impedimento, senza alcun diritto, del funzionamento di un sistema informatico tramite l'introduzione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici>>.

[620] In base all'art.6 della Convenzione, si fa alternativamente riferimento all'intenzionale e senza autorizzazione:

- <<fabbricazione, vendita, approvvigionamento per l'uso, importazione, distribuzione o utilizzabilità in altro modo>>di: <<un'apparecchiatura, incluso un programma per computer>>, ovvero <<una password di un computer, un codice d'accesso, o informazioni simili con le quali l'intero sistema informatico o una sua parte sono accessibili>>, utilizzate per la commissione di almeno uno dei reati menzionati negli articoli precedenti;
- possesso di un elemento menzionato nel punto sopra <<con l'intento di utilizzarlo allo scopo di commettere qualche reato>> menzionato negli articoli precedenti. Si specifica però che non possono essere considerati reato la produzione, distribuzione, vendita, il possesso ed utilizzo degli oggetti menzionati se la finalità non è la commissione dei reati previsti dall'art. 2 all'art.5 della stessa Convenzione.

[621]Traduzioneletterale di <<computer relatedoffences>>: si fa riferimento a tutti quei reati aventi in comune l'utilizzo delle TIC come strumento per la commissione di reati.Ad essi si contrappongono i c.d.<<reati cyber-dipendenti>>(<<computer crimeoffences>>), che identificano invece l'insieme di comportamenti illeciti che prevede l'utilizzo di strumenti elettronici aventi come obiettivo la violazione dell'integrità e della sicurezza dei sistemi informatici (computer compreso) e/o dei dati informatici contenuti in esso.
Per maggiori approfondimenti sul punto, si rinvia a:.UN Office on Drugs and Crime (UNODC), *Computer related-crime,* The Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 18-25 April 2005, Bangkok, Thailand (https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF); AA.VV., *Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, Atti Congresso

c) <<Reati relativi al contenuto>>[624]: si fa riferimento alla disciplina della pedopornografia (art.9)[625]. Vi è anche la disciplina sui reati d'odio, contenuta nel <<Protocollo sugli atti di natura razzista e xenofoba commessi a mezzo di sistemi informatici>> del 2003 .[626]

d) I reati contro la proprietà intellettuale ed i diritti collegati: l'art.10 prevede la necessità di disposizioni penali a tutela della la proprietà intellettuale e del copyright (nonché tutti i diritti legati a quest'ultima) contro l'utilizzo e l'attacco illecito dei sistemi informatici, ponendo però una disciplina in rispetto delle Convenzioni e dei Trattati relativi ai medesimi ambiti[627].

Nella Convenzione di Budapest è previsto anche l'obbligo degli Stati di estensione della responsabilità anche per le persone giuridiche rispetto ai reati summenzionati [628] , precisando comunque che, secondo i principi giuridici dei singoli Stati Parte, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa.

UNODOC Salvador (Brasile) 12-19 aprile 2010(http://unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf); entrambi rinvenibili nel sito ufficiale dell' Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine:https://www.unodc.org/.

[622] In base all'art.7 della Convenzione,la falsificazione informatica consiste nella: <<introduzione, l'alterazione, il possesso o la soppressione di dati informatici derivanti da dati non autentici con l'intento che essi siano presi in considerazione o utilizzati con fini legali come se fossero autentici, senza avere riguardo al fatto che i dati siano o meno direttamente leggibili o intelligibili>>. Si consente per gli Stati la configurazione di questo reato richiedendo anche una condotta fraudolenta.

[623] In base all'art. 8 della Convenzione, la frode informatica consiste nell'intenzionale e senza diritto arricchimento (a vantaggio personale o di terzi) arrecando un danno patrimoniale ad altri, alternativamente: <<con ogni introduzione, alterazione, cancellazione o soppressione di dati informatici>>, ovvero <<con ogni interferenza nel funzionamento di un sistema informatico>>.

[624]Traduzione di <<content-related crime>>, rientrerebbero in questa categoria tutti quei reati relativi al contenuto illecito e /o vietato del materiale prodotto, posseduto o diffuso.

[625] In base all'art.9 comma 1 della Convenzione, si tratta nello specifico de : <<la produzione>>,[…] << l'offerta o la messa a disposizione […] >>, <<la distribuzione o la trasmissione di pornografia infantile allo scopo della sua diffusione attraverso un sistema informatico>>; ;<<il procurare pornografia infantile attraverso un sistema informatico per se stessi o altri>>; <<il possesso di pornografia infantile attraverso un sistema informatico o uno strumento di archiviazione di dati informatici>>.

[626] Il Protocollo si ritrova in: https://www.coe.int/it/web/conventions/full-list?module=treaty-detail&treatynum=189 .

[627]L'art.10 della Convenzione prevede che ogni Parte debba prevedere come reato in base alla propria legge nazionale la violazione della proprietà intellettuale tenendo fede agli obblighi assunti in alcuni atti internazionali, tra cuiil Trattato OMPI sulla proprietà intellettuale, (https://www.wipo.int/edocs/pubdocs/it/wipo_pub_250.pdf); la Convenzione Internazionale per la protezione degli artisti, interpreti ed esecutori, produttori di fonogrammi e organismi di radiodiffusione (c.d. <<Convenzione di Roma>>), https://biblioteche.cultura.gov.it/it/documenti/2018-Aprile-Giugno/ConvenzionediRoma26-10-1961.pdf / . Il terzo comma dell'articolo ammette la possibilità per gli Stati di non prevedere la responsabilità penale in determinati casi, << a condizione che altri rimedi efficaci siano disponibili e che tale riserva non deroghi agli obblighi internazionalmente assunti da questa Parte in applicazione degli strumenti internazionali menzionati […] [in] questo articolo>>.

[628]In base all'art.12 comma 1 della Convenzione, le persone giuridiche sono responsabili di un reato indicato nella Convenzione << commesso per loro conto da una persona fisica che agisca sia individualmente che come membro di un organo di una persona giuridica che eserciti un potere di direzione al suo interno, nei termini che seguono:

a. un potere di rappresentanza della persona giuridica;
b. un'autorità per assumere decisioni nel nome della persona giuridica;
c. un'autorità per esercitare un controllo all'interno della persona giuridica.>>.

Benché questa Convenzione tutt'ora continui ad esser globalmente considerata il modello di riferimento nella lotta contro la criminalità nel mondo cibernetico, di fatto recenti studi hanno segnalato non poche carenze in essa,tutte aventi in comune un unico punto: il fatto che quest'atto, rispetto allo sviluppo tecnologico e cibernetico, sia quasi ormai da considerare <<datato>>[629].

Nello specifico, si rileva che, seppur si riconosca come nella Convenzione venga utilizzato un linguaggio<<tecnologicamente neutro>>[630], in grado di adattarsi perfettamente allo sviluppo tecnologico che avverrà nel corso del tempo (cosa che non sarebbe avvenuta con la scelta dell'utilizzo d'un linguaggio eccessivamente specifico),questa flessibilità di linguaggio rischia però di venire interpretata solo in base al contesto normativo piuttosto che sforzarsi in un linguaggio generali, creando dunque un problema di <<overcriminalizzazione>>[631] delle diverse condotte.

La Convenzione si è poi concentrata sulla condotta criminosa rispetto alla quale sussiste un obbligo di penalizzazione da parte degli Stati, e non tanto sugli strumenti coi quali si esegue la commissione di questi reati: questo ha fatto sì che non pochi meccanismi tecnici sottovalutati ovvero non particolarmente noti ai tempi della stesura della Convenzione non siano stati considerati dalla stessa, seppur oggi invece siano tutt'altro che irrilevanti: un esempio è il botnet[632], strumento utilizzato per tantissime forme diverse di reati cibernetici come, ad es., lo spam, la pedopornografia online e la frode informatica.

Ma non solo: nonostante nel corso degli anni si siano aggiunti (sempre ad opera del Consiglio d'Europa) diversi Protocolli e Convenzioni al fine di coprire ambiti non trattati nella Convenzione Cybercrime[633], vi sono tuttora numerose tipologie di reati manifestatisi

---

[629] Maurushat, *Australia's Accession to the 'Cybercrime Convention': Is the 'Convention' Still relevant in combating Cybercrime in the era of botnets and obfuscation crime tools*?, cit. , in University of New South Wales Law Journal, 2010, Vol. 33, No. 2, pagg. 431-473.

[630]Clough, *op. cit*., pag. 375.

[631] *Ivi,* pag. 376. Con il termine << over-criminalisation>>, s'intende l'eccessivo utilizzo di leggi e regolamenti aventi un effetto dannoso nella società (es. riguardo la realizzazione di condotte incriminatrici che non hanno avuto alcuna vittima).

[632]Il bot è un software utilizzato per infettare un computer, in modo da controllarlo da remoto. Si fa riferimento a :Maurushat, *op. cit*., pag. 438.

[633]Oltre al summenzionato << Protocollo sugli atti di natura razzista e xenofoba commessi a mezzo di sistemi informatici>> del 2003, bisogna citare anche:

- La Convenzione sulla prevenzione del terrorismo (2005) , che tratta anche del reclutamento e dell'addestramento di terroristi tramite Internet (https://www.coe.int/it/web/conventions/full-list?module=treaty-detail&treatynum=196);
- La Convenzione di Lanzarote (2007), che tratta lo sfruttamento sessuale di minori anche online (https://www.coe.int/it/web/conventions/full-list?module=treaty-detail&treatynum=201);

successivamente alla ratifica della Convenzione meritevoli di disciplina per la loro diffusione oramai globale, ma mai ancora considerati. Alcuni esempi sono: il furto d'identità, il c.d. <<grooming>> sessuale[634], lo spam, il cyber terrorismo[635].

Manca poi nell'atto l'individuazione di un organo- regionale, nazionale o sovranazionale che sia - che abbia i poteri necessari per assicurare la corretta ed efficace persecuzione dei reati indicati nella Convenzione da parte di ogni Stato- nonostante le Parti si riuniscano periodicamente al fine di controllare reciprocamente l'applicazione della Convenzione[636].

Come ultimo fattore da tenere in considerazione, emerge nella Convenzionela forte preoccupazione che la ratificazione delle Parti si collochi in due estremi: il predisporre la punibilità per la creazione, distribuzione ed utilizzo dei mezzi creati appositamente solo per la commissione di reati (cosa che creerebbe problematiche nell'ambito dei mezzi di prova); ovvero alternativamente il punire la distribuzione, produzione di tutti i mezzi tecnologici: in quest'ultimo modo l'uso legittimo di essi ovvero la realizzazione di condotte <<con diritto>>[637] sarebbe parimenti incriminato.

- La Convenzione sulla protezione dei dati (1985), la quale pone delle tutele nell'acquisizione ed utilizzo illecito online delle informazioni personali (https://www.coe.int/it/web/conventions/full-list?module=treaty-detail&treatynum=108) .

[634]Per la definizione di <<grooming>> come <<processo tramite il quale il potenziale abusante si guadagna la fiducia del bambino, in modo da poter commettere su di lui successivamente la condotta abusante>>, si veda: Gillespie, *Child Protection on the Internet Challenges for Criminal Law*, cit., in *Child and Family Law Quarterly*, 2002, Vol.14, n.4, pagg. 411-425

[635]Clough, *op. cit*., pagg. 379-387. Nellostessosenso: Id., *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation,* in: *Monash University Faculty of Law Legal Studies Research Paper* , 2015,number 6; *Monash University Law Review*, 2014 Volume 40 number 3, pag. 702.

[636]*Ivi*, pag.703.

[637]*Id*.,*The Council of Europe Convention on Cybercrime,* pag. 376, indica che le condotte eseguite allo scopo di acquisire informazioni per l'analisi dei network ovvero per motivi di sicurezza, rientrano nelle condotte eseguite <<con diritto>>.

2.1.1. La ratifica della Convenzione Cybercrime da parte dell'Italia: la L. n. 48/2008.

L'Italia rientra tra gli Stati che hanno sottoscrittoe ratificato la Convenzione: dopo aver dunque individuato i profili generali di essa, bisogna adesso procedere nell'analisi di come essa sia stata ratificata in Italia e nel vedere se vi siano presenti eventuali problematiche al riguardo (si ricorda -sempre trattando solo il profilo penale sostanziale).

La legge n. 48 del 2008, che ha ratificato la Convenzione, ha rimodellato l'assetto penale in materiacosì come configurato dalla summenzionata l. n. 547/1993[638]. Più precisamente, sulla base delle nuove fattispecie penali introdotte e delle abrogazioni disposte con la legge n.48 del 18 marzo 2008possiamo dividere le novelle in tre grandi gruppi:

1) La falsità informatica e le certificazioni riguardo le firme elettroniche. In esso si trovano: la modifica alla definizione del documento informatico per finalità penali (art. 491 bis c.p.)[639]; l'introduzione nel Libro Secondo del Codice Penale nel Titolo VII relativo ai delitti contro la fede pubblica nel Capo IV concernente <<le falsità personali>> del delitto di false dichiarazioni al certificatore (art.495 bis c.p.)[640]; l'introduzione nei delitti <<contro il patrimonio mediante frode>> (Titolo XIII, Capo II) del delitto di frode informatica del certificatore (art. 640 *quinquies* c.p.)[641];

2) I delitti contro la sicurezza ed integrità dei sistemi. Nell'ordine, si tratta de: la modifica del delitto di diffusione di dispositivi o programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 *quinquies*[642], nel Titolo XII, Capo III, Sez. IV, <<Dei delitti

---

[638]V. *supra* cap. II, par 1.1.

[639]In base all' Art. 3 L. 48/2008,pubblicata anche in *Diritto Penale e Processo,* 2008, n.6 , pag. 696, nell'articolo 491 bis c.p. (<<Documento informatico>>) si aggiunge <<avente efficacia probatoria>> e si sopprime il secondo periodo. Attualmente, all'esito dell'ulteriore riforma del 2016, la fattispecie risulterebbe esser questa: << Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.>>

[640] La disposizione di cui all'art. 495-bis c.p. prevede che: <<Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona, è punito con la reclusione fino ad un anno>>.

[641]La disposizione di cui all'art. 640 *quinquies* c.p. (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica)prevede che: <<Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di arrecare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per un rilascio certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro>>.

[642]Sulla base dell'art. 4 L. 48/2008,l'art. 615 *quinquies* è stato così modificato:<<Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a

contro l'inviolabilità del domicilio>>); la modifica del delitto di danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.[643], in: Titolo XIII, Capo I, <<Dei delitti contro il patrimonio mediante violenza alle cose o alle persone>>); l'introduzione del delitto di danneggiamento dei sistemi informatici (art. 635-quater c.p.[644], nel Titolo XIII, Capo I <<Dei delitti contro il patrimonio mediante violenza alle cose o a persone>>); l'abrogazione del delitto d'attentato informatico (art. 420^{2-3} c.p.[645]), e l'inserimento dei delitti di danneggiamento di informazioni, dati e programmi informatici di pubblica utilità (art. 635-ter c.p.[646]) ed il danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.[647]), entrambi nel Titolo XIII, Capo I;

3) L'estensione della responsabilità penale per tutti i delitti informatici (e non solo, dunque, per quelli summenzionati) alle persone giuridiche tramite il nuovo articolo 24-bis del Decreto Legislativo numero 231 del 8/6/2001[648].

---

due anni e con la multa sino a euro 10.329>>. Importante segnalare che questa norma è stata modificataulteriormente dalla l. n. 238/2021 , la quale ha ampliato la sua portata applicativa estendendo la punibilità non più esclusivamente alla detenzione di sistemi, apparecchiature o programmi volti al danneggiamento, ma anche alla loro distribuzione ed installazione abusiva.

[643]Sulla base dell'art.5^{1} della L.48/2008, il comma 1dell'art. 635-bis c.p. è il seguente:<<Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con reclusione da sei mesi a tre anni>>.

[644] Sulla base dell'art.5^{2} della L.48/2008, la disposizione dell'art. 635-quater è: << Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni>>.Il secondo comma di questo articolo, come modificato dalla l. n. 7/2016 è ora il seguente: "Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata."

[645]Si fa riferimento all'art.6, L. 48/2008.

[646]Sulla base dell'art.5^{2} della L.48/2008 e a seguito dell'ulteriore modifica dell'ultimo comma ad opera della l. n. 7/2016, la disposizione del 635-ter è: <<Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata >>.

[647]Sulla base dell'art.5^{2} della L.48/2008 e a seguito dell'ulteriore modifica dell'ultimo comma ad opera della l. n. 7/2016, la disposizione dell'art. 635-quinquies è la seguente: << Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata >>.

[648] In base dell'art.7 della L. 48/2008 , la disposizione dell'art. 24^{1-2}-bis del D.Lgs. 231/2001 risulta essere: <<In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote>>.

Definiti i punti principali di questa legge di ratifica, si cercherà di approfondire alcuni tra i diversi articoli modificati, abrogati ed introdotti con essa, anche allo scopo di fare emergere criticità di carattere generale della disciplina; in seguito si concluderà questo sottoparagrafo verificando se vi sia stata una piena ratifica della Convenzione di Budapest da parte della legge 48/2008, sulla base di quanto trattato finora.

Partendo dalla materia della falsità informatica, s'eseguirà la trattazione di due articoli relativi alla tematica delle firme elettroniche, in particolare soffermandosi sul rapporto tra il soggetto <<che esercita servizi di certificazione>>[649] e l'utilizzatore di essi.

Bisogna iniziare dal delitto di false dichiarazioni al certificatore (art. 495-bis c.p.),che punisce il soggetto che esegue un'attestazione o dichiarazione con firma elettronicanon veritiera o genuina su <<l'identità o lo stato o altre qualità della propria o dell'altrui persona>>[650]rivolta al certificatore. Questo reato è inseritotra i delitti <<contro la falsità personale>> (e non al Capo precedente, il Capo III, riguardante i delitti contro la <<falsità in atti>>).

Eseguendo un paragone con l'articolo di falsa attestazione o dichiarazione ex art. 495 c.p.[651], è opportuno notare che, mentre per la configurazione dell'art. 495 c.p. è necessario che la dichiarazione o attestazione venga eseguita davanti ad un pubblico ufficiale, nell'art.495-bis invece si fa riferimento al <<soggetto che presti servizi di certificazione delle firme elettroniche>>.
Questa distinzione potrebbe far emergere la volontà del Legislatore del 2008 di escludere la natura pubblicistica del certificatore: se fosse però effettivamente così, si negherebbe che la stessa attività dei certificatori abbia il compito di tutelare anche la c.d. <<"pubblicità legale" da garantire alle chiavi pubbliche>> [652] tramite verifica della corrispondenza dell'identità del soggetto e della firma digitale posta sui documenti- tratto che non si può non considerare di natura pubblicistica.

In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote >>.
[649] Picotti, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Diritto Penale e Processo*, 2008, n.6, pag. 704.
[650] Art. 495-bis c.p.
[651] Si riporta in questa nota il contenuto dell'art. 495[1] c.p.: <<Chiunque dichiara o attesta falsamente al pubblico ufficiale l'identità, lo stato o altre qualità della propria o dell'altrui persona, è punito con la reclusione da uno a sei anni.>>
[652] *Ivi,* pag. 706.

A sostegno della natura pubblicistica del certificatore, si deve poi guardare anche il profilo sanzionatorio: se il certificatore avesse un ruolo puramente privatistico, perché mai l'art. 495-bis dovrebbe allora prevedere una misura sanzionatoria molto più grave rispetto alla falsa dichiarazione eseguita ad un pubblico ufficiale (ovvero un incaricato di un pubblico servizio nell'esercizio delle sue funzioni), ex art. 496 c.p. ?

Curiosamente, anche il reato di frode informatica al certificatore (art 640-quinquies c.p.) ha una particolare collocazione, al pari del delitto precedente: come si è già detto, è stato collocato tra i delitti contro il patrimonio mediante frode (Titolo XII, Capo II).
Questo reato riguarda la figura del certificatore, che <<al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare un danno, viola gli obblighi previsti dalla legge rilasciando un certificato qualificato>>.

Comparando l'analisi di questa disposizione con il reato di frode ex art. 640 c.p.[653] (l'articolo di riferimento per la norma in analisi), emergono non poche differenze: rispetto a quest'ultima, nell'art. 640-quinquies manca l'aspetto dell'artifizio e del raggiro, nonché non è essenziale in alcun modo che vi sia un evento lesivo del patrimonio altrui (se nella frode si prevede espressamente <<ingiusto profitto *con* altrui danno>>[654], nell'articolo in esame si parla invece di <<un ingiusto profitto *ovvero* di arrecare un danno>>). In sintesi, in questa fattispecie <<la mera […] violazione di obblighi extrapenali>>[655] al fine di perseguire un interesse proprio o altrui risulterebbe essere più che sufficiente per la consumazione del reato.

Oltre ad essere molto distante nella sua struttura rispetto al resto delle fattispecie collocate in questo Titolo e Capo, emergerebbe dunque che essa si qualificherebbe più come<<un'incriminazione meramente "sanzionatoria" della violazione di obblighi extrapenali, gravanti in specie su soggetti qualificati, […]>>[656] che come reato lesivo di beni giuridici meritevoli di tutela penale: ciò farebbe sorgere dei dubbi sulla correttezza della previsione della rilevanza penale di questa fattispecie.

---

[653]Si riporta qui l'art. 640[1]c.p. :<<Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sè o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032>>.
[654]Si veda la nota sopra.
[655]Picotti, *op. cit*., pag. 707, fa riferimento agli obblighi previsti per il Certificatore nel Codice dell'Amministrazione Digitale, art. 32[2] e commi seguenti.
[656]*Ibidem.*

Riguardo alla materia dei danneggiamenti informatici, bisogna accennare al fatto che il Legislatore italiano, in conformità alla Convenzione Cybercrime, ha eseguito uno scernimento tra i danneggiamenti di dati ed i danneggiamenti di sistemi, distinguendoli poi ulteriormente ~~i~~n base al fatto se i dati o sistemi danneggiati siano privati o di dominio privato: vengono dunque create quattro tipologie di danneggiamento informatico.
Da un raffronto tra le fattispecie emergono plurime criticità, di cui si farà qualche breve cenno:

Cominciando dal delitto di danneggiamento di dati informatici (art 635-bis c.p.), in esso risulterebbe esser presente quella che verrebbe definita <<l'innovazione maggiore>>[657] di questa legge del 2008, ossia l'inserimento della procedibilità tramite querela dell'offeso - spiegabile come un tentativo del Legislatore di abbassare il numero oscuro delle vittime di queste tipologie di reato[658].

Vi è però un punto che suscita un particolare dubbio nella lettura di questa fattispecie: non è particolarmente chiara quale sia la persona offesa. Considerato che i dati ed i programmi informatici non possono aver la stessa disciplina giuridica delle cose materiali, basarsi solo sulla <<altruità dei dati danneggiati>>[659] - sufficiente per reati come il danneggiamento di cose ex art. 635 c.p. - non risulta centrare l'obiettivo della loro corretta e concreta identificazione.
Ma non c'è solo questa problematica: è stata tralasciata nella norma la menzione del concetto <<senza diritto>> - presente invece frequentemente negli articoli della Convenzione del Cybercrime.

C'è un'altra critica da fare anche sul fatto tipico della fattispecie in esame: nella norma emerge la punibilità delle condotte di chi <<[…] distrugge, deteriora, cancella altera o sopprime informazioni, dati o programmi informatici […] >>[660], mentre il Legislatore non menziona in alcun modo nella norma la condotta del danneggiare.
Considerato che il danneggiamento di una cosa può comportarne l'inservibilità, si potrebbe supporre che - relativamente al danneggiamento di dati e programmi informatici – la condotta di danneggiamento potrebbe corrispondere a quelle attività che rendano

[657]Picotti, *op. cit*., pag. 710.
[658]Riguardo quest'aspetto, si rinvia al punto 1.3. di questo capitolo, relativo alla parte del profilo generale delle vittime di cybercrime.
[659]*Ivi*, pag. 711.
[660]Art. 635-bis c.p. .

(temporaneamente o meno, <<inaccessibili i dati>>[661]): per cui, perché non inserirla come condotta penalmente punibile?

Si potrebbe pensare che quest'omissione sia una scelta del Legislatore di restringere <<l'ambito del penalmente rilevante>>[662]: in realtà, bisogna notare che la stessa condotta del <<danneggiare>> è menzionata nell'art. 634-quater c.p.(il danneggiamento di sistemi informatici o telematici). Inoltre, se effettivamente il Legislatore italiano avesse voluto compiere una scelta del genere, egli piuttosto avrebbe previsto nell'articolo la punibilità solo per quelle condotte che <<determinano danni seri>> [663] come indicato nella Convenzione. In base a quanto detto finora, quest'ipotesi è dunque da escludere, e rimane persistente la nebulosità della *ratio* di questa curiosa scelta da parte del Legislatore.

Bisogna poi fare un breve cenno ai delitti di danneggiamento contro i dati informatici di pubblica utilità (635-ter c.p.) e contro i sistemi informatici o telematici di pubblica utilità (635-quinquies). Aspetto interessante è comprendere la ragione per cui il legislatore ha voluto distinguere queste due fattispecie da quella vista sopra e dall'art. 635-quater (il danneggiamento di sistemi informatici o telematici).
Nell'art. 635-ter si prevede come condizione necessaria l'utilizzazione dallo Stato o da altro Ente pubblico dei dati o dei programmi informatici[664], mentre nell'art. 635-quinquies non si fa altro riferimento se non alla <<pubblica utilità>>. Oltre a questo, non vi sarebbero altre indicazioni su quale sarebbe <<rapporto di pertinenza con lo Stato ed un ente pubblico, specie nella […] grande indeterminatezza dei […] diritti ed interessi convergenti su dati, informazioni e programmi>>[665].

Vi è dunque una critica da muovere nei confronti del Legislatore per la poca chiarezza con cui ha eseguito questa distinzione tra dati ed informazioni ovvero sistemi di carattere privato ovvero pubblico in autonome fattispecie,considerato che gli articoli 635-ter e 635-quinquies non solo non prevedono delle circostanze aggravanti speciali, ma anche hanno il medesimo sistema sanzionatorio rispetto agli articoli 635-bis e 635-quater.

---

[661] Picotti, *op. cit*., pag. 712.
[662] *Ibidem.*
[663] Convenzione di Budapest, Art.4[2], pag. 4.
[664] Si ricorda, nell'art. 635-ter[1] c.p. la locuzione :<<chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, […]>>
[665] Picotti, *op. cit.,* pag. 715.

Se da un lato non si comprende perché il Legislatore abbia eseguito questa distinzione non presente nella Convenzione, dall'altro lato occorre rilevare che non ha invece prestato attenzione ad un aspetto essenziale indicato dalla Convenzione stessa: il riportare nella legge di ratifica la distinzione tra il danneggiamento di dati ed il danneggiamento di sistemi.

Ultimo reato da affrontare relativo alla materia è l'art. 615-quinquies, ossia il reato di diffusione di dispositivi o programmi volti a danneggiare o interrompere un sistema informatico- non rientrante nelle quattro disposizioni penali di danneggiamento menzionate precedentemente, ma meritevole comunque di menzione per le caratteristiche peculiari che presenta dopo la sua riformulazione tramite la legge 48/2008.

Presentandosi negli anni '90 sempre più di frequente le situazioni di creazione, vendita, distribuzione ed utilizzo di virus informatici allo scopo di eseguire attacchi informatici, la Convenzione ha previsto la punibilità nell'abuso di apparecchiature che fossero concepite o adattate per la commissione esclusiva di fini illeciti; nonché l'accesso abusivo[666] (uso di codici per l'accesso illecito ad un sistema informatico) - come si è già avuto modo di vedere.

Guardando l'attuale disposizione dell'articolo 615-*quinquies* del codice penale, questa precisazione sulla Convenzione permette di cogliere meglio due grandi diversità:

- Solo la nozione di accesso abusivo indicata nella Convenzione è confluita nell'articolo in questione,
- Viene indicato solo lo scopo di danneggiamento illecito dei programmi nella disposizione, mentre non è indicato in alcun modo che i programmi o i dispositivi siano <<diretti>> al danneggiamento.

  Quest'ultimo punto affronta quello che è il punto fondamentale della problematica di quest'articolo: se nella Convenzione di Budapest la pericolosità o dannosità della condotta è sul piano oggettivo, nella legge italiana del 2008 questa pericolosità si è spostata <<nel contenuto della finalità "soggettiva" dell'agente>>[667]- focalizzatasi solo sul dolo specifico, ossia lo scopo effettivo perseguito dall'autore del reato.

[666]Si fa riferimento, nell'ordine: art. 6 par. 1 e 2, pag.4 della Convenzione di Budapest.
[667]Picotti, *op. cit.,* pag. 709.

In conclusione, questa scelta di base del Legislatore italiano di fondare la punibilità dell'art. 615-quinquies <<sul *solo* elemento finalistico >>[668] non soltanto va in <<una direzione diametralmente opposta a quella tracciata nella Convenzione>>[669], ma per giunta realizza un enorme rischio - percepito già nella redazione della Convenzione stessa:in questo modo si rischierebbe appunto di perseguire penalmente qualsiasi utilizzo di apparecchi, dispositivi, programmi o codici per l'accesso (totale o parziale) a sistemi o dati informatici o telematici, anche nel caso in cui la condotta sia posta in essere<<con diritto>> ovvero per la persecuzione di una finalità lecita.

Infine, trattando brevemente la responsabilità da reato degli enti per i delitti informatici, a parte poche incongruenze non del tutto chiare – come l'esclusione della responsabilità penale per la frode informatica se il delitto non è commesso <<in danno dello Stato o di altro ente pubblico>>[670], e per la falsa attestazione al certificazione ex art. 495-bis c.p. - risulta che l'art. 12 della Convenzione abbia trovato piena attuazione nel Decreto Legislativo del 2001. Vi è tuttavia un piccolo aspetto da sottolineare su questa tematica: estendendo l'applicazione dell'obbligo per le persone giuridiche di avere un modello organizzativo adeguato a prevenire anche i reati informatici, si rende in questo modo ancora più complesso il sistema di adattamenti e precauzioni che l'impresa deve adottare – e si può aggiungere anche dispendioso, considerata la rapida evoluzione delle diverse forme di reato cibernetico e delle loro modalità d'esecuzione.

Giunti a tirare le fila del discorso nella disamina della Legge 48/2008, viene fatto notare come, da queste incongruenze riscontrate nella trattazione dei vari articoli, emerga la frettolosità del Legislatore italiano in questa legge.
Oltre alla straordinaria rapidità con cui questa legge fu progettata, discussa ed approvata con un consenso quasi unanime dalle Camere[671], si vuol porre all'attenzione sul fattoche pure gli stessi parlamentari fossero consapevoli di queste problematiche. Confidando però

[668] *Ivi,* pag. 710.
[669] *Ibidem.*
[670] Picotti, *op. cit.,* pag. 716, fa riferimento all'art. 24[1] D.Lgs. 231/2001 : << In relazione alla commissione dei delitti di cui agli articoli 316-bis, 316-ter, 356, 640, comma 2, n. 1, 640-bis e 640-ter secommesso in danno dello Stato o di altro ente pubblico odell'Unione europea, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote. >>
[671] Sulla base di quanto detto da: Picotti, *op. cit*., pag. 700, il disegno di legge viene presentato nel giugno del 2007, ed in un giorno solo la Camera dei Deputati (19 febbraio 2008) discute, conclude e trasmette il testo al Senato, il quale, in poche ore, eseguirà il passaggio nelle commissioni del testo, la discussione ed approvazione definitiva nel 27 febbraio 2008.

nel lavoro interpretativo della magistratura e ritenendo prioritario l'adeguamento dell'ordinamento italiano al sistema internazionale, esse hanno preferito - rispetto a queste nuove forme di reati - disporre la medesima disciplina rivolta alle fattispecie penali preesistenti (come si è visto, ad es., col reato di frode informatica) ed approvare velocemente la legge piuttosto che soffermarsi ulteriormente sulla formulazione del progetto di legge e sulla sua discussione.

Pertanto,si può dire che l'Italia abbia effettivamente adempiuto ad una piena ed efficace ratificazione della Convenzione in conformità all'ordinamento internazionale, in base agli artt. 10, 11 e 117 Cost.?La risposta parrebbe enunciarsi più in forma negativa per diverse ragioni.

Innanzitutto, bisogna rivolgere una critica all'eccessiva leggerezza delle Camere nella formulazione della Legge esaminata: bisogna ricordare infatti che la chiarezza e precisione di una norma giuridica sono aspetti fondamentaliin un ordinamento di Civil Law (come quello italiano) - a maggior ragione per il diritto penale, considerato il principio di legalità ex art. 25 Cost.
Per cui, è necessario dedicare i tempi necessari nell'iter legislativo e non delegare il <<grosso>> del lavoro all'attività interpretativa dei magistrati.
Inoltre, come si è potuto ben vedere anche nel paragrafo precedente, la materia dell'informatica e della cibernetica presenta sì analogie, ma prevalentemente forti peculiarità e diversità rispetto al mondo <<reale>>: era dunque necessaria molta più attenzione al tema, facendo <<un approfondito esame delle diverse fattispecie penali preesistenti e dei riflessi sistematici di ogni modifica>>[672].

In conclusione, questa legge può essere considerata solo un parziale adempimento del pieno recepimento della Convenzione, nonché dell'obbligo di cooperazione internazionale e dell'armonizzazione legislativa: si auspica perciò una revisione della Legge 48/2008 in questione da parte del Legislatore, con una maggior presa di consapevolezza dell'attualità e della rilevanza di una materia così complessa e mutevole come quella oggetto di questa trattazione.

[672]Picotti, *op. cit*., pag. 716.

2.2. I diversi approcci nel mondo al fenomeno Cybercrime: cenni sugli altri strumenti internazionali in materia.

Anche se, come detto precedentemente, l'adesione alla Convenzione di Budapest era aperta anche a Stati diversi dai membri del Consiglio d'Europa,ad oggi[673]sarebbero solo 68gli Stati che hanno aderito ad essa (di cui 2 di essi -Sud Africa ed Irlanda –non hannoancora ratificato), quindi alla Convenzione non hanno aderito tutti gli Stati del mondo–ma soltantocirca un terzo degli Stati presenti globalmente (198), anche a ragione della lunghezza e complessità del processo di accesso [674].

A questo punto, è naturale chiedersi - in linea di massima -quali possono essere gli altri strumenti legislativi di tutela contro i crimini cibernetici ed informatici a disposizione degli altri Stati non sottoscriventi la Convenzione di Budapest.

La risposta si cercherà di trovarla in questo punto della trattazione e nel successivo, ma c'è un'importante premessa di carattere comune da svolgere: tendenzialmente, un livello minimo di tutela viene fornita dalla Convenzione di Palermo (in particolare, in riferimento agli artt. 18-19-20[675], riguardanti la cooperazione giudiziale ed investigativa sui fenomeni di criminalità organizzata).

Tuttavia, seppur la Convenzione di Palermo sia considerata tuttora uno dei mezzi più efficaci a livello internazionale contro <<i fenomeni criminali collettivi>> (compresi quelli

---

[673] Si veda: Clough, *The Council of Europe Convention on Cybercrime,*pag.387.

[674]Come indicato da Clough, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, pag. 724, innanzitutto, l'accesso dello Stato terzo deve avvenire tramite previo apposito invito del Consiglio d'Europa, ma per diventare definitivamente membro della Convenzione è necessario un voto favorevole di maggioranza del Comitato dei Ministri del Consiglio d'Europa, nonché l'unanimità degli Stati Membri. Si segnala anche un'interessante osservazione eseguita sul punto da**:** Maroz*, Regionalization of International cooperation in the fightagainstCybercrime*, in *Law Review*(Romania), 2019, vol.X, Issue 2, a pag. 224, secondo cui questa scelta di seguire un procedimento così complesso è in pieno contrasto con la scelta di porre in essere una Convenzione che - come detto precedentemente – possa esser sottoscritta anche da Stati non membri del Consiglio d'Europa: questa caratteristica, propria di un trattato di carattere più <<locale>>, farebbe perciò escludere la natura unitaria ed universale della Convenzione di Budapest.

[675] Sabbatini*, La Convenzione di Palermo ed i negoziati per il rafforzamento della cooperazione internazionale*, in Rivista di Studi e Ricerche contro la Criminalità Organizzata, 2019, Volume 5, numero 4, pagg. 50 (DOI: http://dx.doi.org/10.13130/cross-13095/), parla appositamente del *ReviewMechanism*, che interverrebbe anche sugli articoli menzionati, allo scopo di raggiungere questi obiettivi:

- << realizzare con i paesi terzi, estranei all'Unione Europea, nuove forme di cooperazione giudiziaria, indispensabili per contrastare fenomeni criminali aventi natura globale;
- superare gli ostacoli che si frappongono alla raccolta delle prove in paesidove le istituzioni dello Stato attraversano un difficile processo di ricostruzione, mentre vaste zone del territorio sono sotto il controllo di organizzazioni criminali impegnate in molteplici attività delittuose, dal traffico dei migranti al commercio illegale di armi e di stupefacenti;
- predisporre un quadro di standard internazionali che rafforzino la funzionalità, e al tempo stesso le garanzie, per le nuove tecniche investigative rese necessarie dall'evoluzione tecnologica>>;

non espressamente indicati in essa, ma che non hanno ancora formato oggetto di <<analoghi strumenti internazionali>>[676]); essa non può esser considerata sufficiente per una piena tutela rispetto a qualsiasi tipologia di crimine informatico e cibernetico: sia perché limitata ai soli fenomeni di crimine organizzato transnazionale commessi in rete ex art. 3p.1 della Convenzione[677], sia perché si è rilevato che vi possono essere delle stesse problematiche nell'applicazione di una cooperazione giudiziale e di poliziastabile se gli Stati membri non hanno ancor prima <<una base giuridica adeguata che ne consenta l'impiego su obiettivi situati all'estero>>[678].

Inizialmente,gli Stati esteri non erano propensi alla formazione di un'unitaria Convenzione in tema di cybercrime da parte delle Nazioni Unite a cui aderire. Questo ha fatto sì che, da un lato, vi sia stata la creazione nel corso degli anni di numerose Convenzioni[679] per garantire dei parametri legali generali e sufficienti per affrontare un fenomeno transnazionale come il Cybercrime; e,dall'altro lato,che si sia riscontratal'urgenza per gli Stati d'assumere, per proprio conto, ulteriori atti legislativi aventi ad oggetto l'azione penale contro il Cybercrime, validi ed efficaci solo nei territori delle Parti aderenti ad essi. Come si può facilmente intuire, questo ha creato non poca frammentazione.

Secondo un quadro generale, queste tipologie di trattati <<locali>> contro i crimini cibernetici ed informatici si possono dividere in due macrogruppi:

1. Il primo è stato (in parte) trattato: corrisponde alla Convenzione di Budapest, ma anche a quei trattati <<locali>> che si sono formati prendendo come riferimento la stessa. Si tratteranno nel dettaglio due degli esempi più eclatanti.

---

[676]Sabbatini, *op.cit*., pag. 39.

[677] Riportando la disposizione sovracitata dal testo della Convenzione (https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf), pag.6: <<La presente Convenzione si applica, salvo disposizione contraria, alla prevenzione, investigazione e all'esercizio dell'azione penale per: (a) I reati stabiliti ai sensi degli artt. 5, 6, 8 e 23 della presente Convenzione; e (b) I reati gravi, come da art. 2 della presente Convenzione; laddove i reati sono di natura transnazionale e vedono coinvolto un gruppo criminale organizzato.>>

[678]Sabbatini, *op. cit*., pag. 51.

[679]Maroz*, op. cit.*, a pag.221, indicache dal 2010 al 2017 sono state poste in essere circa seiConvenzioni: la *African Union Convention on Cyber Security and Personal Data Protection*, cit., nel 2014 (https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection/); *The Protocol on Interaction of the Member States of the Collective Security Treaty Organization in counteracting criminal activity in the information security area*, cit., del 2014 (https://en.odkb-csto.org/);*The agreement on cooperation of the State Parties of the Commonwealth of Independent States in fight against crimes in the field of computer information*, ,nel 2001 (https://cis-legislation.com/document.fwx?rgn=4129); *Arab Convention on Combating Information Technology Offences, cit.,* nel 2010 (https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf).

Il primo è la c.d. <<Arab Convention on Combating Information Technology Offences>>, posta nel 2010 sulla base della Convenzione di Budapest. Il trattato è principalmente composto da due parti: la prima parte è rivolta all'<<armonizzazione della legislazione penale, sia dal punto di vista processuale che sostanziale>>, mentre la seconda si concentra sulla cooperazione legale e giurisdizionale.

Vi sono alcuni vantaggi rispetto alla Convenzione di Budapest in quest'atto: il più eclatante è l'inserimento nella parte sostanziale di tutta una serie di figure di reato legate ai reati informatici non presenti nella Convenzione (es. il traffico umano, il cyber terrorismo, ecc.). Dall'altro lato, però viene rilevato un difetto di carattere non trascurabile: viene notato che spesso viene imposto alle Parti l'obbligo di prevedere una certa condotta come reato, senza però dare una chiara indicazione di quello che sia il fatto tipico[680].

Il secondo esempio è invece l'<<African Union Convention on cyber security and personal data protection>> del 2014: come l'esempio precedente, ha il vantaggio di mostrare molta più accuratezza nella parte penale sostanziale - specie riguardo ai <<content related crime>>[681] e gli attacchi contro i sistemi informatici.

Tuttavia, questa Convenzione ha tratti lacunosi con riguardo all'ambito dell'assistenza e cooperazione legislativa delle Parti: sulla base dell'art.28 della Convenzione, gli Stati membri che non hanno particolari accordi sull'assistenza legale reciproca nella materia dei reati cibernetici verrebbero incoraggiati a stipulare con altri Stati ulteriori accordi internazionali, allo scopo di regolare la tematica[682].

2. Il secondo macrogruppo include, invece, due tra i trattati creati storicamente dopo lo scioglimento dell'URSS, il Protocollo del CSTO (<<Collective Security Treaty Organization >>) contro i crimini nell' area della sicurezza informatica (<<The Protocol on Interaction of the MemberStates of the Collective Security Treaty Organization in counteractingcriminalactivity in the information security area>>) del 2014, nonché l'Accordo del Commonwealth sui reati relativi alle Tecnologie dell'Informazione e Comunicazione (<<The agreement on cooperation of the State Parties of the

[680] *Ivi,* pag. 225, fa riferimento diretto alla Convenzione Araba, artt.13-14, pag.7, dove, per le descrizioni per l'obbligo di porre come reati *<<altre forme di pornografia>>* e i reati *<<contro la privacy>>*, si dispone rispettivamente *<<lo sfruttamento sessuale>>* e *<<offese contro la privacy con l'uso di qualsiasi mezzo tecnologico>>*.

[681] Per la definzione, si rinvia al punto 2.1. nella trattazione della Convenzione di Budapest.

[682] Si riporta qui la disposizioneoriginale dell'art.28 dellaConvenzione, par. 2: <<State Parties that do not have agreements on mutual assistance on cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance with the principle of double liability […]>>.

Commonwealth of IndependentStates in fightagainstcrimes in the field of computer information>>)del 2001.

Questi trattati – seppur in zone geografiche molto distanti tra loro - hanno in comune diversi aspetti: l'interesse di guardare di più all'obiettivo dell'armonizzazione legislativa in materia penale piuttosto che al coordinamento e alla cooperazione giudiziale[683]; una particolare attenzione per individuare gli strumenti giuridici necessari per contrastare i reati nel settore tecnologico ed informatico; e la presenza di una posizione internazionale piuttosto omogenee [684]-seppur questo non comporti per gli Stati un conflitto d'interessi relativamente alle obbligazioni assunte da entrambi gli atti.

Gli atti internazionali in questione però divergono sul loro contenuto: il Protocollo è focalizzato sul fornire un quadro legislativo forte per la repressione in materia penale di tre specifiche condotte, considerate come illecite in concordanza al Protocollo stesso (<< [le condotte] contro il Sistema Costituzionale e la sicurezza dello Stato>>, << [le condotte] contro la pace e la sicurezza dell'umanità>>, << [le condotte] nell'ambito delle informazioni tecnologiche>>[685]); mentre l'Accordo del Commonwealth non contiene granché né sulle previsioni riguardo i reati informatici, né sull'armonizzazione del profilo processuale rispetto all'utilizzo di prove elettroniche; tuttavia, compensa il fatto che in esso vi sia un'estesa trattazione della cooperazione legislativa relativamente ai reati nell'ambito delle TIC.

Da una veloce rassegna di alcuni esempi di misure internazionali contro il fenomeno del cybercrime, si può dunque ben intuire che la nascita di questi numerosi e diversi atti internazionali sul medesimo tema ed allo stesso tempo di contenuto altamente specifico e circoscritto a determinati ambiti, sia stata la causa principale della nascita della c.d. <<regionalizzazione della cooperazione internazionale>>[686]: una situazione non poco ambigua, considerata la natura transnazionale dei reati cibernetici ed informatici.

Se, da una determinata angolazione, questi differenti approcci di livello sovranazionale possono esser la soluzione ideale per affrontare situazioni di reati cibernetici ben localizzati; allo stesso tempo un'eccessiva suddivisone crea un ostacolo non indifferente

[683]Maroz, *op. cit.*,pag. 221.
[684]Come indicato da:*Ivi,* pag. 222, gli Stati aderenti ad entrambi gli atti internazionali sono: l'Armenia, il Belarus, la Federazione Russa, il Kazakistan, il Tagikistan, il Kirghizistan.
[685]Si è eseguita tradizione del concetto espresso da:*Ibidem.*: [conduct] << against consitutional system and state security, against peace and security of mankind, in the field of information tecnology>>.
[686]*Ivi,*pag. 227.

sia per l'applicazione giurisprudenziale che per il coordinamento legislativo, nonché per la cooperazione della polizia e per l'estradizione.

Inutile dire che tutto ciò è un risultato più che vantaggioso peri cybercriminali, poiché questa situazione crea un <<paradiso sicuro>>[687] per loro, che possono agire indisturbati, aumentando ancor di più la loro consapevolezza di non esser mai individuati e condannati per i reati da loro commessi.

Questo panorama finora descritto permette anche di arrivare ad un'altra importante considerazione, ossia che la Convenzione sul Cybercrime del Consiglio d'Europa non è uno strumento in grado di realizzareda solo un'unitaria azione penale ed universale contro il fenomeno dei reati cibernetici.Ciò nonostante, non si deve rinunciare alla individuazione e previsione di parametri coerenti ed unitari nel panorama internazionale relativamente all'azione penale contro i crimini cibernetici: oltre al fatto che si ridurrebberoenormemente i contrasti giurisprudenziali, legislativi, nonché le problematiche di coordinamento e cooperazione tra Paesi, rimane evidente che, data la <<aterritorialità>> della rete, risulta essere piuttosto difficile (se non addirittura impossibile) agire efficacemente contro questa tipologia di reati senza un quadro normativo internazionale e sovranazionale solido e correttamente applicato dalle Parti.

2.3.Il futuro progetto di una Convenzione ONU sul Cybercrime: breve analisi e confronto dei diversi progetti prospettati da Stati Uniti, Regno Unito, Russia e Cina.

L'indispensabilità di un panorama legislativo e giurisprudenziale unitario e coeso, in grado di rimettere nuovamente in gioco << la battaglia contro il crimine informatico>>e che sia al contempo in grado di porre gli strumenti necessari <<nell'ottica di una possibile armonizzazione a livello globale>>[688]è una problematica sicuramente nota (specie dopo la venuta della pandemia, che ha innalzato le percentuali di attività criminali online nel mondo a livelli mai visti finora[689]).

---

[687]*Ivi,*pag. 221.

[688]Mattarella, *La futura Convenzione ONU sul Cybercrime ed il contrasto alle nuove forme di criminalità informatica*, in Sistema Penale, 2022, Vol. 3, pag. 58 (https://www.sistemapenale.it/it/articolo/convenzione-onu-cybercrime/)

[689] Per maggiori approfondimenti sul punto, si cita: Sleiman, Gerdemann, *Covid-19: a catalyst for cybercrime?*, in *International Cybersecurity Law Review* , 2021, vol. 2, Issue 1, pagg. 37–45; Travaini,

Non si può dire allo stesso modo, però, che vi sia un'idea condivisa unanimemente dagli Stati sulla tipologia di contenuto dell'atto internazionale bastevole per raggiungere questi obiettivi,visto che da anni si discute sul piano internazionale con non poca fatica su queste tematiche: basti fare un accenno al fatto che, durante il Dodicesimo Congresso delle Nazioni Unite sulla prevenzione del crimine e sulla giustizia criminale del 2010[690], si era creata una vera e propria divisione di opinioni sulla decisione o meno di prendere iniziativa sul piano internazionale e incominciare a negoziare per una nuova Convenzione contro il Cybercrime.

Vi era chi, come la Russia o la Cina, erano favorevoli a questa opzione, ma erano più numerosi gli Stati contrari all'idea (Unione Europea, Stati Uniti, Inghilterra), i quali sostenevano che la Convenzione di Budapest fosse già lo strumento internazionale sufficiente per contrastare questo fenomeno, per cui essa doveva esser utilizzata come base per <<il potenziamento delle sue capacità e per creare maggiore consapevolezza>>[691] a livello globale.

Tuttavia, questa <<spinta>> mossa dalla Russia e dalla Cina non fu vana: fu creato presto un gruppo intergovernativo sulla criminalità informatica (il c.d. IEG)[692], e la Russia, nel 2017, ha presentato una bozza di convenzione sulla criminalità informatica alle Nazioni Unite. Nonostante quest'ultima iniziativa della Russia sia sfociata con successo nel 2019 nella Risoluzione 74/247, essa è stata accettata <<senza votazione, in base ad un'accettazione generale>>[693] solo in seguito agli emendamenti presentati dai vari Stati, che, seppur diversi tra loro, avevano in comune il fatto che volevano un procedimento più trasparente, con un maggior coinvolgimento della popolazione.

Nel 2022 è ufficialmente iniziata la fase dei negoziati per la Convenzione, e si auspica che la Convenzione venga adottata ad inizio 2024: tuttavia, come si intuirà dalle diverse

---

Caruso, Merzagora, *Crime in Italyat the time of the pandemic,* in *Acta bio-medica: Atenei Parmensis*, 2020, vol. 91, Issue 2, pagg.199-203. DOI:10.23750/abm.v91i2.9596; Monteith, Bauer, Alda, Geddes, Whybrow, Glenn, *Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry*, in *Current Psychiatry Rep*ort, 2021, Volume 23, Issue 4, pagg. 18-27. DOI:10.1007/s11920-021-01228-w.

690 AA.VV., *Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, Atti Congresso UNODOC Salvador (Brasile) 12-19 aprile 2010, pag.56.

691Clough, in *The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World*, a pag.388 riprende una definizione emersa nell'Assemblea del Quintetto dei Procuratori Generali provenienti da Australia, Nuova Zelanda, Canada, Inghilterra e Stati Uniti: AA.VV., *Quintet of Attorneys General Action Plan to Fight Cyber Crime'*, in US Reference Service, 2011, http://usrsaustralia.state.gov/us-oz/2011/07/15/aag2.html .

692Mattarella, *op. cit.*, pag. 59.

693Per maggiori approfondimenti sul tema dei negoziati: Walker, Tennant, *Control, alt or delete? The UN Cyber crime debate enters a new phase,*in Global Initiative against transnational organized crime, December 2021 (https://globalinitiative.net/wp-content/uploads/2021/12/UN-Cybercrime-PB-22Dec-web.pdf)

posizioni di alcuni Paesi sulle tematiche che verranno trattate, il raggiungimento di una soluzione accolta complessivamente sul contenuto ed obiettivi di questa futura Convenzione sembra ancora un obiettivo piuttosto lontano.

Iniziando dagli Stati Uniti, per gli stessi è fondamentale che venga posta in essere una Convenzione in grado di frenare la criminalità informatica, ma allo stesso tempo prevedendo garanzie e limiti per la tutela dei diritti umani (nello specifico, sui temi de <<l'assistenza tecnica e della cooperazione degli Stati in […] ausilio dei paesi dotati di minori risorse tecnologiche>>[694]).

Vi è poi un'interessante osservazione da svolgere: a parere degli Stati Uniti, questa Convenzione deve avere come contenuto solo la definizione delle condotte illecite nel cyberspazio e delle rispettive sanzioni (ad es. la distinzione tra i reati cyber-dipendenti e cyber-correlati[695]), mentre si deve invece escludere la trattazione nell'atto della sicurezza informatica. Questo perché, nella visione statunitense, se la prima è di sola responsabilità degli Stati membri, la seconda è invece di <<responsabilità condivisa di una serie di attori pubblici e privati>>[696]: di conseguenza, la Convenzione deve solo limitarsi a definire quali sono le condotte dei cybercriminali e le rispettive sanzioni,senza dettare le norme comportamentali degli operatori in ambito informatico.

Altro aspetto che gli Stati Uniti hanno particolarmente evidenziato è stata la neutralità del linguaggio che dovrebbe essere usato nella Convenzione: considerato il costante evolversi della tecnologia, è necessario che le disposizioni possano mantenere la loro applicabilità nel corso del tempo.

Per far questo, occorre che le fattispecie s'incentrino sull'attività illecita posta in essere che mette in pericolo <<la riservatezza, l'integrità e disponibilità dei dati informatici>>[697], piuttosto che invece guardare allo strumento utilizzato- ragione per cui questo Paese sollecita l'introduzione di nuove fattispecie di reato nell'atto internazionale, come ad es. l'accesso illegale ad un computer o sistema informatico senza autorizzazione, le frodi informatiche (come il phishing), l'intercettazione illecita di dati tramite attacchi Denial of Service ovvero ramsonware, la cancellazione o modifica dei dati.

[694]Mattarella, *op. cit.*, pag. 60.
[695]Per la definizione di entrambi, si richiama al punto 2.1. nella trattazione della Convenzione Cybercrime.
[696]Mattarella, *op. cit.*, pag. 60.
[697]*Ivi.*, pag. 61.

Relativamente agli aspetti della visione statunitense elencati finora, risulta che il Regno Unito sia aderente in tutti i punti elencati precedentemente. Infatti, anche per questo Stato, il futuro accordo deve, nell'ordine: usare un linguaggio tecnologicamente neutrale affinché non siano necessari frequenti aggiornamenti dell'atto, indicare gli scopi della normativa e le definizioni da utilizzare, recepire la distinzione tra reati cyber-dipendenti e reati cyber-correlati. Infine, non dovrebbe rientrare nella Convenzione la materia della sicurezza informatica.

Tuttavia, questo Stato è ugualmente meritevole di autonoma menzione per due specifiche ragioni. La prima è l'importanza che viene conferita a questo futuro atto internazionale come mezzo <<di rafforzamento della cooperazione>>[698] non solo tra Stati, ma anche per le imprese ed i cittadini: il Regno Unito, nella sua relazione, evidenzia come carattere essenziale che la futura Convenzione debba essere conforme alle disposizioni previgenti delle Nazioni Unite in materia penale (specie alla Convenzione di Palermo ed alla Convenzione di Merida del 2005 contro la corruzione), poiché è vitale <<costruire un sistema normativo coerente>>[699].

La seconda ragione è la pressione per l'imprescindibile presenza nella Convenzione di garanzie che tutelino i diritti umani ed il rispetto della privacy, come riconosciuto dalle numerose risoluzioni adottate dalle Nazioni Unite. Tra le varie tematiche in questione, si fa un accenno in particolare alla necessità di porre in esseremeccanismi in grado di rifiutare l'estradizione per violazione del ne bis in idem, se la condotta illecita in questione è legata <<all'esercizio della libertà di espressione>> e <<la richiesta di consegna ha lo scopo di punire o perseguitare l'individuo per motivi di razza, religione, sesso o motivi politici>>[700].

In sintesi, l'Inghilterra richiede che per la stesura di questo nuovo accordo internazionale venga utilizzato un approccio inclusivo e aperto anche ai cittadini, società private, aziende, istituzioni accademiche.

Se questi due Stati hanno una visione pressoché simile, altrettanto non si può dire invece della relazione presentata dalla Russia, un documento molto complesso ed articolato.

[698] *Ivi.*, pag. 62.
[699] Mattarella, *op. cit.*, pag. 63.
[700] *Ibidem.*

Per questo Stato è fondamentale che nell'atto vengano trattate come priorità <<l'assistenza tecnica, il rafforzamento delle capacità di prevenzione degli Stati e l'aumento del livello di sicurezza delle informazioni>>[701].

Si trova una singolarità già nella premessa, in quanto v'è un particolare interesse alla tutela della sovranità: secondo la Russia, non solo la Convenzione non può interferire col principio di sovranità e di non ingerenza negli affari interni dei diversi Stati, ma essa non può nemmeno consentire che l'Autorità di uno Stato Parte della Convenzione possa esercitare in un altro Stato Parte la propria giurisdizione (o altre funzioni relative al diritto interno dello Stato stesso).

Ad evidenza della consapevolezza della diffusione di questi crimini, nella parte sostanziale vi è un lavoro analitico e svolto con particolare cura da parte della Russia nell'individuazione delle fattispecie penali.

Dandone una breve schematizzazione, viene richiesto nella Convenzione l'inserimento de:

- Le fattispecie minaccianti la sicurezza: ad es., l'accesso non autorizzato alle informazioni o dati personali, l'intercettazione, l'interferenza o interruzione di reti, la creazione di distribuzione o utilizzo di software dannosi;
- Le fattispecie di reati informatici legate alla tutela di soggetti vulnerabili: ad es. la pedopornografia, l'istigazione o coercizione al suicidio;
- Le fattispecie di reato commesse nel cyberspazio allo scopo di diffusione di <<ideologie disumane e antidemocratiche>>[702]: ad es., i reati connessi all'estremismo ed al terrorismo, i reati d'odio;
- I principali traffici illeciti commessi dalle organizzazioni criminali in via transnazionale (lo spaccio di stupefacenti, il traffico d'armi e di esseri umani)- a testimonianza del riconoscimento del forte legame tra il cybercrime e la criminalità organizzata;

In chiusura, si segnalano due articoli della relazione russa meritevoli di particolare attenzione: l'articolo 26, che identifica la possibilità per gli Stati di adottare le misure necessarie per reprimere l'uso delle tecnologie per la commissione di atti considerati reati dalla Convenzione (lasciando ferma, ex art. 29, la possibilità per ogni Parte di <<sanzionare qualsiasi condotta illecita, non rientrante nella Convenzione, commessa

[701] *Ivi*,pag. 66.
[702] Mattarella, *op. cit.*, pag. 68.

attraverso l'uso intenzionale di mezzi tecnologici e che provochi danni significativi>>)[703]; nonché l'art. 30 , che prevede la configurabilità di una responsabilità degli enti giuridici per i reati cibernetici, con un forte riaggancio alla disciplina presente nell'art. 10 della Convenzione di Palermo[704].

Si chiude il quadro trattando la posizione della Cina, incentrata sull'esigenza della prevenzione: secondo questo Stato,la futura Convenzione deve avere in sé gli strumenti necessari per monitorare ed impedire il più possibile la formazione di nuove forme di reato cibernetiche, mantenendo <<una base giuridica flessibile>>[705].

Nello specifico, riguardo alla parte di dirittopenale sostanziale, è necessario che vengano considerate penalmente illecite tutte le attività costituenti <<la "catena" delle operazioni illecite>>[706] (atti preparatori compresi), e si suggerisce di fornire criteri per determinare la giurisdizione dei diversi reati, considerata la peculiarità del ciberspazio. Nel contempo, è necessario che gli Stati predispongano degli strumenti essenziali per ideare le manovre politiche necessarie per consentire un maggior controllo e protezione rispetto ai crimini del ciberspazio.

Successivamente, la Cina evidenzia due punti nella sua relazione: la necessità di predisporre ulteriori misure processuali per la cooperazione internazionale (specie riguardo la raccolta di prove elettroniche transfrontaliere), nonché l'esigenza di predisporre elementi chiave per garantire tutela contro i crimini cibernetici sono indubbiamente l'assistenza tecnica e lo scambio di informazioni (<< la formazione di operatori giudiziari e di polizia, l'istituzione di gruppi di esperti […], lo sviluppo delle tecniche di indagine elettronica, e la fornitura di attrezzature e tecnologie>>).[707]

---

[703]*Ibidem.*

[704]Si riporta qui l'intera disposizione dell'art. 10 della Convenzione Di Palermo: <<Ogni Stato Parte adotta misure necessarie, conformemente ai suoi principi giuridici, per determinare la responsabilità delle persone giuridiche che partecipano a reati gravi che coinvolgono un gruppo criminale organizzato e per i reati di cui agli artt. 5, 6, 8 e 23 della presente Convenzione.
Fatti salvi i principi giuridici dello Stato Parte, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa. Tale responsabilità è senza pregiudizio per la responsabilità penale delle persone fisiche che hanno commesso i reati. Ogni Stato Parte si assicura, in particolare, che le persone giuridiche ritenute responsabili ai sensi del presente articolo siano soggette a sanzioni efficaci, proporzionate e dissuasive, di natura penale o non penale, comprese sanzioni pecuniarie.>>

[705]Mattarella, *op. cit.*, pag. 69.

[706]*Ibidem.*

[707]*Ivi*, pag. 70.

Da quanto visto finora, si può dunque percepire la presenza di due poli opposti: il primo è formato da Russia, Cina e da altri Stati dell'Est Europa (in testa l'Ungheria), che vedono necessario ripartire da nuova Convenzione *ad hoc*; il secondo dall'Europa Occidentale, dal Regno Unito e dagli Stati Uniti, più interessati a creare un <<doppio binario>>: uno rivolto ad una chiara delineazione dei poteri pubblici tenuti a << prevenire e punire il crimine cibernetico>>, l'altro invece è relativo alla sicurezza, materia lasciata <<ad una maggiore libertà dei soggetti privati>>[708]- non disdegnando affatto per questo compito l'utilizzo della Convenzione di Budapest come traccia di riferimento.

Come primo punto conclusivo si puònotare che la problematica di fondo sull'utilizzo della Convenzione già esistente come standard per la stesura della nuova ovvero sulla necessità di ricominciare *ex novo* sia ancora presente da più di dieci anni.Nonostante l'accuratezza delle idee presentate, difficilmente sarà possibile arrivare ad una fase conclusiva della nuova Convenzione se non si supera questo ostacolo.

Secondariamente, quale potrebbe essere il possibile contenuto della Convenzione? Secondo i più recenti studi[709], si sono prospettate quattro possibili scenari per l'esito dei negoziati:

1) La nuova Convenzione sia posta in piena adesione alla proposta della Russia: se si scegliesse questa strada, si vedrebbe un aumento esponenziale della presenza politica della Cina e della Russia a livello internazionale in quest'ambito. Tuttavia, visto il forte accento sulla sovranità statale, si tende a sottolineare come questa visione sia eccessivamente restrittiva dei diritti umani e della libertà di espressione online, nonché foriera di non pochi ostacoli alla cooperazione internazionale.

2) La seconda ipotesi possibile è di carattere opposto: la nuova Convenzione potrebbe essere una versione molto più estesa della Convenzione di Budapest. Seguendo questa via, si avrebbero i benefici di garantire l'aumento delle tutele previste per i diritti umani e di avere una maggiore approvazione da parte del settore privato, che avrebbe un maggiore campo d'azione. Vi sono però anche degli svantaggi: quello di maggior rilevanza è che si perderebbe l'appoggio di potenze internazionali, compromettendo la cooperazione internazionale.

[708] *Ivi*,pag. 66.
[709] Si fa riferimento a Walker, Tennant*, op.cit*., pag. 24.

3) Una terza via potrebbe essere quella della mediazione: gli Stati potrebbero accordarsi sul linguaggio utilizzato nella Convenzione e sulle terminologie, lasciando poi ad ogni autorità nazionale ampio spazio interpretativo. In questo modo, si avrebbe un atto internazionale di carattere flessibile e molto probabilmente adottato globalmente (similmente alla Convenzione di Palermo). È essenziale, tuttavia, che si preveda un meccanismo di revisione efficace, in grado di <<aumentare la trasparenza generale nella lotta alla criminalità informatica>>[710], anche per controllare e studiare il suo effettivo impatto.

4) Un ultimo possibile esito è che le Parti siano talmente irremovibili nelle loro posizioni da impedire il raggiungimento di un accordo, lasciando <<la cooperazione internazionale sulla lotta alla criminalità informatica>>[711]ancora più frammentata di prima.

Difficile dire quale tra le ipotesi prospettate si avvicinerà di più all'effettivo contenuto della futura Convenzione. Una cosa è però certa: tutti i partecipanti alle riunioni per la progettazione del futuro accordo internazionale sono ben consapevoli di quanto sia indispensabile arrivare alla sua formazione, visto il raggio d'estensione sempre più grande dei reati cibernetici

[710]Mattarella, *op. cit.*, pag. 74.
[711]*Ivi,* pag. 75.

2.4. La dimensione sovranazionale. La rilevanza della criminalità informatica nell'art 83 TFEU e le recenti iniziative dell'Unione Europea.

La problematicità della natura <<aterritoriale>> della rete è stata percepita anche nell'ordinamento dell'Unione Europea: seppur anch'essa sia soggetto Parte della Convenzione di Budapest ed avendo essa stessa spinto gli Stati Membri alla sua ratificazione[712], il quadro legislativo fornito dal sistema europeo ha dei tratti caratteristici tali da esser meritevoli di una trattazione a parte.

Per quanto la materia del diritto penale europeo sia ampia e complessa[713], è opportuno fare un sintetico quadro storico. Prima del Trattato di Lisbona, si parlava al massimo di un c.d. <<diritto penale comunitario in senso debole>>[714], ossia un diritto europeo in cui non erano previste delle sanzioni, e dive venivano posti precetti non vincolanti per gli Stati Membri[715]. Sarà solo grazie alla rivoluzionaria decisione giurisprudenziale della Corte di giustizia del 2005 nel c.d. "*environmental crime case*" che si affermerà la necessità che il diritto europeo si occupi anche della materia penale, attraverso strumenti in grado d'imporsi agli Stati Membri e di rafforzare la cooperazione di polizia e giudiziaria[716], seguita poi dall'adozionedel Trattato di Lisbona del 2007-inquadrante la competenza

---

[712] Come indicato in: Picotti, *La nozione di <<criminalità informatica>> e la sua rilevanza per le competenze penali europee*, in *Riv. Trim. dir. Pen. Econom*., 2011, vol.4, pag. 860.

[713] Per maggiori approfondimenti, sulla competenza penale dell'Unione europea, si cita: Camaldo, *La Competenza penale europea dopo il trattato di Lisbona,* in Id. (a cura di), *L'istituzione del procuratore europeo e la tutela penale degli interessi finanziari dell'unione europea*, Giappichelli Editore, 2014; Picotti, *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona,* in: Sicurella et al., *L' evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona,* Pubblicazioni del Centro di Diritto Penale Europeo (Catania), 2011, pagg. 207-233; Riondato, *Competenza penale della Comunità europea. Problemi di attribuzione attraverso la giurisprudenza,* CEDAM, 1996.In generale, v., di recente, i vari contributi contenuti in: Grandi (a cura di), *I volti attuali del diritto penale europeo*, Pisa, 2021.

[714] Donini, *Integrazione Europea e Scienza Penale*, in *Riv. Trim Dir. Pen. Econom*,2020, vol. 3-4, pag. 535.

[715] Andando più nel dettaglio come indicato da Picotti, *op. cit.,* pag. 856 e ss., si trattava della struttura dei c.d. Pilastri (relativamente alla materia penale, si parlava nello specifico del III Pilastro), che consentiva tramite le Decisioni Quadro di predisporre misure minime di ravvicinamento del diritto dei vari Stati Membri- crimini informatici compresi, anche se <<non esplicitamente menzionata nei Trattati>>.

[716] Si fa riferimento alla sentenza della Corte di Giustizia Europea del 13/09/2005,Causa C-176/03(https://eurlex.europa.eu/legalcontent/IT/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A2005%3A542),nelle pagg. I-7915, I-7916, in cui si riporta espressamente che la Commissione Europea, nei verbali di dichiarazione di adozione delle decisioni quadro in materia di reati contro l'ambiente, ha riportato che: << […] la decisione quadro non sia lo strumento giuridico idoneo con cui obbligare gli Stati membri ad introdurre sanzioni di carattere penale a livello nazionale […]>>; nonché che<<[…] nell'ambito delle competenze attribuitele ai fini del raggiungimento degli obiettivi di cui all'articolo 2 del Trattato che istituisce la Comunità europea, la Comunità abbia facoltà di obbligare uno Stato membro ad imporre sanzioni a livello nazionale — se del caso anche penali —, qualora ciò risulti necessario ai fini del raggiungimento di un obiettivo comunitario>>.

penale europea tramite l'utilizzo delle direttive -, e dell'art. 83 TFUE[717], il quale in linea definitiva consacra una competenza europea in materia penale–autonoma, indiretta econcorrente con quella degli Stati Membri- nel predisporre le misure minime e necessarie ("norme minime relative alla definizione dei reati e delle sanzioni")per la repressione de <<la criminalità di << dimensione transnazionale>>>>[718], consentendo una <<unificazione delle competenze penali europee nell'ambito del quadro comunitario>>[719] tramite le direttive.

Più in dettaglio, l'inserimento tra <<le sfere di criminalità>>particolarmente gravedi dimensione transnazionale anche della criminalità informatica[720] comporta due novità fondamentali:

1) In primo luogo, viene esteso non poco il raggio d'azione della competenza penale europea nella materia, prima limitata al massimo all'ambito della criminalità organizzata o al terrorismo (es. decisione quadro 2005/22 contro gli attacchi informatici);

2) Viene richiesto un attivo controllo del Parlamento Europeo e dei Parlamenti Nazionali nella formulazione ed adozione di atti legislativi (dalla Corte di Giustizia Europea e dalle Corti Nazionali di grado più elevato, invece, sul piano giurisdizionale) al fine di rispettare i principi di sussidiarietà e di proporzionalità, nonché un controllo sui limiti indicati nella stessa norma dell'articolo 83 TFEU: la finalità di stabilire <<norme minime>> di ravvicinamentodelle legislazioni penali degli Stati membri; nonché la natura <<grave>> e <<transnazionale>> della criminalità e la necessità di predisporre basi comuni per combatterla.

Riguardo la nozione della <<criminalità informatica>> inserita nella norma, ci si è chiesto se essa riguardi solo i reati informatici in senso stretto ovvero anche quelli in senso lato ed

[717]Riportando qui l'intero testo dell'articolo 83 (1), del Trattato sul Funzionamento dell'Unione Europea (C-202), pubblicato (in versione aggiornata) ne La Gazzetta Ufficiale de L'Unione Europea del 07/06/2016 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C:2016:202:FULL), pagg. 80-81: <<Il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono 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.
Dette sfere di criminalità sono le seguenti: terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata.
In funzione dell'evoluzione della criminalità, il Consiglio può adottare una decisione che individua altre sfere di criminalità che rispondono ai criteri di cui al presente paragrafo.
Esso delibera all'unanimità, previa approvazione del Parlamento europeo.>>
[718]Donini*, op. cit.,* pag. 536.
[719]Picotti, *op. cit*., pag. 858.
[720]Si fa espresso richiamo alla nota precedente relativa alla disposizione dell'art. 83 TFUE (1).

i reati cibernetici; ma non risulterebbero esservi particolari dubbi nell'orientarsi per la seconda ipotesi: sia per la già menzionata adesione alla Convenzione di Budapest dell'Unione, sia perché, posto che lo stesso articolo 83 TFUE è stato introdotto allo scopo di ampliare la competenza penale europea e riprende lo scopo, già presente nei precedenti Trattati della Comunità europea,di emanare <<norme minime di ravvicinamento>>[721], è difficile infatti pensare che questa frase venga interpretata in via restrittiva.

Facendo poi un confronto anche con le altre sfere di criminalità menzionate nel paragrafo 1 dell'articolo 83 TFUE, possono emergere delle problematiche nella collocazione giuridica di reati informatici o cibernetici relativi ai medesimi argomenti (es. il riciclaggio di denaro in rete). A questa possibile situazione bisogna applicare il criterio di specialità riguardo alla tipologia di criminalità da contrastare: se è più accentuato l'aspetto tecnologico, si deve guardare alla criminalità informatica; in caso contrario, si dovrà riferirsi a quelle tipologie di criminalità <<che nella valutazione legislativa sembrino <<assorbire>> siffatto elemento in connotati diversi e ritenuti più specifici>>[722].

Bisogna poi fare un breve riferimento anche al paragrafo 2 dell'art. 83 TFUE che prevede la c.d. competenza penale accessoria dell'Unione europea[723]: considerando che esso ha una formulazione volutamente elastica[724]e - a differenza del paragrafo precedente - non sono presenti i requisiti della gravità e transnazionalità ma solo quello della mera <<necessità>> della disciplina penale a livello europeo, è ben possibile che in futuro emergano potenziali conflitti di competenza europea tra il primo ed il secondo paragrafo dell'art. 83 TFEU(il che ha conseguenze, ad esempio, sulla procedura legislativa da seguire per l'approvazione della Direttiva) – considerando,a maggior ragione, la diversità delle discipline in cui possono emergere nuove tipologie di reati cibernetici o informatici (es. la violazione della proprietà intellettuale di opere postate in rete). Come è stato però correttamente

[721]Come indicato da Picotti, *op. cit*., pag. 860, seppur la locuzione sia presente nell'art. 83 (2) TFUE, essa era anche tra le competenze europee del III pilastro.
[722] *Ivi*, pag. 862.
[723] Si riporta qui la disposizione dell'art. 83 (2)TFUE: <<Allorché il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri in materia penale si rivela indispensabile per garantire l'attuazione efficace di una politica dell'Unione in un settore che e` stato oggetto di misure di armonizzazione, norme minime relative alla definizione dei reati e delle sanzioni nel settore in questione possono essere stabilite tramite direttive. Tali direttive sono adottate secondo la stessa procedura legislativa ordinaria o speciale utilizzata per l'adozione delle misure di armonizzazione in questione, fatto salvo l'articolo 76>>.In argomento v.Bernardi, *La competenza penale accessoria dell'Unione europea: problemi e prospettive,* in *Dir. pen. cont*. – *Riv. Trim*., 2012, pag. 21 ss.
[724]Come indicato da Picotti, *op. cit*., pag. 862, la *ratio* legislativa è stata di <<dotare le <<politiche>> e le fonti extrapenali dell'Unione europea di strumenti sanzionatori efficaci, seguendo parametri di ragionevolezza e proporzione <<in concreto>> rispetto allo scopo di attuazione equivalente in tutto il territorio europeo>>.

osservato[725] , il problema non è risolvibile solo con l'utilizzo del criterio di specialità, ma bisogna osservare anche la diversità dei requisiti indicati tra il primo ed il secondo paragrafo dell'articolo: si parlerà di <<criminalità informatica>> ex art.83 p.1 TFEU solamente se non solo è prevalente l'aspetto tecnologico nel reato, ma anche se sono presenti i requisiti della transnazionalità e gravità menzionati nel primo paragrafo dell'articolo indicato pocanzi.

In base alla descrizione eseguita finora, si può dunque ben comprendere perché quest'articolo sia stato la base per introdurre strumenti idonei a promuovere la prevenzione e repressione a livello uniforme della criminalità transnazionale- reati cibernetici ed informatici compresi-, garantendo allo stesso tempo cooperazione tra gli Stati Membri e le diverse Istituzioni Europee.

In via di chiusura di questo paragrafo, si intende brevemente soffermarsi su quale è stata (e quale potrebbe diventare) la via intrapresa a livello europeo,partendo da quest'articolo, per la tutela dei propri cittadini e delle rispettive Istituzioni relativamente alla materia del Ciberspazio.Si possono in proposito citare alcuni atti legislativi europei relativi al tema ed attualmente in vigore.

Oltre alle Direttive che, pur dirette a reprimere particolari forme di criminalità, considerano anche l'aspetto informatico (come, ad es., la Direttiva 2011/93/UE, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e la Direttiva 2019/713/UE, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti),vi è anzitutto da menzionare laDirettiva 2013/40 UE contro gli attacchi ai sistemi informatici e telematici: il provvedimento, posto in sostituzione della Decisione Quadro 2005/222 GAI e sulla spinta della Convenzione di Budapest,si fonda sulla considerazione che <<il buon funzionamento e la sicurezza dei sistemi di informazione siano fondamentali per lo sviluppo del mercato interno e di un'economia competitiva e innovativa >>[726] . Punto centrale di questo provvedimento è l'obiettivo che tutti gli Stati Membri predispongano misure penali che siano << effettive,

[725]*Ivi*, pag. 863.
[726]Conigliaro, *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della nuova direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *Archivio Diritto Penale Contemporaneo* 2013, pag. 1
https://archiviodpc.dirittopenaleuomo.org/upload/1383078657CIVELLO%20CONIGLIARO%202013a.pdf

proporzionali, dissuasive>>[727] contro gli attacchi ai sistemi informatici- ferma restando la possibilità d'intervento dell'Unione in base al principio di sussidiarietà ex art. 5 TUE.

Gli aspetti più noti di questa direttiva a cui il sistema penale italiano nel tempo ha dovuto adattarsi sono:

- l'inserimento tra gli<<strumenti utilizzati per commettere i reati>> anche del possesso di<< codici d'accesso che permettono di accedere in tutto o in parte a un sistema di informazione>>[728] ;
- Riguardo alla fattispecie di creazione o diffusione di strumenti idonei alla commissione di un attacco informatico, per l'Italia emerge l'esigenza di inserire nelle fattispecie penali corrispondenti (artt. 615-ter e quater c.p.) elementi che consentano di verificare che l'intenzione con cui questi strumenti vengono utilizzati sia quella di commettere un reato, in modo da evitare la persecuzione di condotte lecite;
- la previsione dell'obbligo per gli Stati d'incriminare la condotta illecita d'intercettazione di comunicazioni[729]: esso ha imposto in Italia l'aggravamento delle misure sanzionatorie dell'art. 615-quater c.p., nonché la rimozione del dolo specifico di <<trarre profitto e di arrecare danno>> [730] nel summenzionato articolo, poiché restringente <<l'ambito di punibilità più di quanto permesso dagli obblighi di tutela penale derivanti dall'art. 83 TFUE>>[731].

Vi è poi tutto un quadro normativo recentemente posto per la tutela della sicurezza cibernetica. Elencando alcuni atti di riferimento, si cita: la Direttiva europea NIS (Network

[727]Si fa riferimento al punto 33 delle Premesse nella Direttiva 2013/40/UE, pubblicata nella Gazzetta Ufficiale dell'Unione Europea del 14.08.2013, a pagina L218/11 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32013L0040).
[728]Art. 7 punto b) della Direttiva 2013/40/UE a pag. L218/12 .
[729]Art. 6 della Direttiva summenzionata a pag. L218/12, di cui si riporta qui la disposizione:<<Gli Stati membri adottano le misure necessarie affinché l'intercettazione, tramite strumenti tecnici, di trasmissioni non pubbliche di dati informatici verso, da o all'interno di un sistema di informazione, incluse le emissioni elettromagnetiche da un sistema di informazione che trasmette tali dati informatici, compiuta intenzionalmente e senza diritto, sia punibile come reato, almeno per i casi che non sono di minore gravità>>.
[730]Conigliaro*, op .cit.*, pag. 5, fa riferimento a: Trib. Milano, 28/09/2007,in *Foro ambrosiano*, 2007, pag.325.
[731]*Ibidem.*

and Information Security) 2016/114[732], il Regolamento generale sulla protezione dei dati personali n. 679/2016[733] ed il c.d. Decreto Cybersecurity (il Reg. UE 2019/881[734]).

Nel 2023 è entrata in vigore anche la Direttiva NIS2 (Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione), che abroga la precedente Direttiva NIS e amplia l'ambito di applicazione delle norme in materia di sicurezza dei dati, potenziando gli organi e le attività di supervisione a livello comunitario, con l'obiettivo di migliorare la collaborazione per contrastare la minaccia informatica globale, anche attraverso la razionalizzazione dei requisiti minimi di sicurezza e delle procedure di notifica obbligatoria degli incidenti informatici.

Sotto questo profilo,si può vedere la più recente presa di posizione dell'Unione Europea: piuttosto che prevedere nuove fattispecie di reato a cui gli Stati devono conformarsi, si è preferito imporre delle misure obbligatorie <<agli operatori di determinati servizi essenziali>> (es. nei settori di trasporto o bancari), ossia <<misure tecniche e organizzative di prevenzione>> e <<obblighi di comunicazione alle autorità degli attacchi informatici che incidono sulla continuità dei servizi>>[735] . La logica orientante questa scelta è stata indubbiamente l'aumento esponenziale in Europa sia degli attacchi informatici negli ultimi anni,sia della vendita di mezzi con cui commettere queste tipologie di attacchi[736]: era dunque urgente trovare un sistema che tutelasse le Istituzioni (europee e nazionali), le Pubbliche Amministrazioni ed i cittadini davanti a questa nuova minaccia.

Si aggiunge poi che, in vista della futura Convenzione ONU, la Commissione Europea di recente ha annunciato che proporrà a breve una revisione di numerose direttive e decisioni[737]concernenti diverse tematiche, ma tutte legate al sistema cibernetico (es. la

[732]Direttiva UE 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, in Gazzetta Ufficiale dell'Unione Europea del 19/07/2016, pagg. L.194/1- L.194/30, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148 .

[733] Regolamento UE 2016/679 del Parlamento europeo e del Consiglio (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati), in Gazzetta Ufficiale dell'Unione Europea del 04/05/2016.

[734]Il Regolamento menzionato (Reg. UE 2019/881) è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 7/06/2019, pagg. L 151/15 - L 151/69, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=PT .

[735]Mattarella, *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Diritto penale e processo*, 2022, vol.6, pag. 820.

[736]Guastella, *Il dominio geopolitico dello spazio cibernetico*, 2020, Edizioni Ex Libris, pag. 123 e ss.

[737]Mattarella, *op. cit.,* menziona: la Dir. 2014/42/UE, relativa al congelamento e alla confisca dei beni strumentali e dei proventi da reato nell'Unione europea (pubblicata in Gazzetta Ufficiale dell'Unione Europea il 29/04/2014, pagg. L 127/39- L 127/50, https://eur-lex.europa.eu/eli/dir/2014/42/oj/ita/pdf); la

cooperazione tra gli uffici degli Stati membri peril recupero dei beni relativi al reperimento ed identificazione dei proventi di reato, l'attività di ricerca di indizi e prove - specie nell'ambito delle intercettazioni -, e nell'ambito delle informazioni finanziarie).

Inoltre, parrebbe anche esser piuttosto forte la pressione europea nella creazione di una rete di servizi segreti in grado di individuare più velocemente le informazioni relative alle attività svolte dalla criminalità organizzata operante online - area anch'essa in costante crescita[738].

In conclusione, anche l'Unione Europea è impegnata a trovare strumenti unitari efficaci contro le minacce del Cybercrime, ma allo stesso tempo questi strumenti devono esser anche in grado di resistere ai diversi mutamenti socio-economici del tempo:

- da un lato, è necessario creare un modello di cooperazione tra soggetti pubblici e soggetti privati, in grado di punire le nuove forme di reato, ma anche di predisporre strumenti e modelli di controllo efficaci (in particolare per le persone giuridiche);
- dall'altro lato, la repressione del Cybercrime deve avvenire nel rispetto della sfera privata dei cittadini (il diritto alla privacy), nonché di tutti gli altri diritti fondamentalipropri del singolo cittadino europeo.

In sostanza, all'Unione è ben chiaro che in questa lotta a queste nuove forme di reato bisogna agire eseguendo un bilanciamento dei vari interessi pubblici e privati in gioco, in modo da evitare che <<la lotta alle nuove forme di criminalità vanifichi le conquiste e le possibilità, anche in termini di libertà, offerte dal cyberspazio>>[739].

Decisione 2007/ 845/GAI del Consiglio (pubblicata in Gazzetta ufficiale dell' Unione europea il 18/12/2007, pagg. L 332/103 - L 332/105, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32007D0845); nonché la Dir. UE 2019/1153 del Parlamento europeo e del Consiglio (pubblicata in Gazzetta Ufficiale dell'Unione Europea l'11/7/2019, pagg. L186/122- L186/137, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019L1153).

[738] Per maggiori approfondimenti sul punto, si fa direttamente richiamo a: Ruggiero, *Crimine organizzato e transnazionale in Europa*, in *Studi sulla questione criminale*, 2015,Vol. 2-3, pagg. 183-201, doi: 10.7383/84447.

[739]Mattarella, **op. cit*., pag. 829.

3. L'impatto del cyberspazio sul diritto penale italiano: profili critici.

Si è accennata nel paragrafo iniziale del capitolo[740] la scelta del Legislatore Italiano di introdurre le fattispecie penali (sia quelle nate interamente nel cyberspazio, sia quelle già esistenti, ma che possono esser attuate anche nel cyberspazio) nella parte speciale del Codice Penale, piuttosto che creare una sezione apposita. Inoltre, si è voluto far notare, nel paragrafo precedente, come la sceltadi mero ricalco delle fattispecie preesistenti non si sia rivelata vincente, <<data la difficoltà di far rientrare fatti, condotte od oggetti profondamente diversi in schemi concepiti per realtà differenti>>[741].

Il mondo cibernetico ha messo in forte discussione il sistema penale italiano, sia con riguardo sia alla parte speciale (le tipologie di fattispecie penali modificate ovvero introdotte, nonché l'emersione di nuovi beni giuridici da tutelare[742]) che a quella generale, in non pochi istituti basilari e strutturanti la figura del reato.Non si approfondiranno tutti i singoli aspetti in questa sede perché meritevoli di una trattazione approfondita che non può esser svolta in quest'elaborato. Per dare completezza all'argomento trattato in questo capitolo,è comunque opportuno soffermarsi su taluni specifici aspetti.

Innanzitutto, si è dovuto ripensare alla nozione di fatto tipico e di evento[743], nonché alla consumazione del fatto stesso. Considerando la caratteristica dell'automazione[744] dei sistemi informatici e cibernetici, non si possono non tenere in conto quegli eventi e quei fatti che avvengono automaticamente in esecuzione di programmi complessi, seppur il sistema cibernetico o informatico utilizzato dal soggetto per la commissione del reato.

Inoltre, la potenziale permanenza dei dati nel tempo e nello spazio fa sì che il fatto tipico non si realizzi pienamente al momento del suo perfezionamento, ma solo <<al suo esaurimento sostanziale>>[745], ossia alla piena cancellazione dei dati dal sistema (difficile, ma non impossibile il suo avverarsi). Da quanto detto finora, si comprende quindi sia come il confine tra le distinzioni dei due concetti di condotta ed evento sia del tutto

---

[740]Si fa riferimento al Paragrafo 2.1., *Il passaggio dai reati informatici ai reati cibernetici*.

[741]Picotti, *Sistematica dei reati informatici tecniche di formulazione legislativa e beni giuridici tutelati,* in Picotti,*Il diritto penale dell'informatica nell'epoca di Internet*, CEDAM, 2005, pag. 53.

[742]Per maggiori approfondimenti sul punto, si cita: Picotti, *Sistematica dei reati informatici*, pagg. 21 e ss.

[743]Riportando la nozione di fatto tipico, si fa riferimento all'insieme degli elementi estrinseci con cui si manifesta il reato (la condotta umana, gli eventuali presupposti del fatto, il nesso di causalità e l'evento - inteso quest'ultimo comeleconseguenze di un'azione od omissione che costituisce reato).

[744]Sul significato si fa richiamo espresso a al Paragrafo 2.1., *Il passaggio dai reati informatici ai reati cibernetici.*

[745]Picotti, *Diritto Penale e tecnologie informatiche: una visione d'insieme*, *cit.,*pag. 92.

instabile, sia come nell'individuare il momento di consumazione del reato sidovrà tenere conto di questa<<fase ulteriore di "prolungamento">>[746].

Conseguentemente, l'attenzione cade anche sul nesso di casualità: se è fatto indubbio la <<persistente disponibilità dei contenuti illeciti online>>[747], vi sono diverse opinioni sul riconoscere o meno una rilevanza penale alla fase temporale in cui il contenuto illecito permanga in rete[748], al fine di rilevare se, ai fini della sussistenza del nesso causale, sia bastevole la condotta dell'autore del reato ovvero sia necessaria anche la permanenza degli effetti della sua condotta in Rete.

A ciò si aggiunge anche la problematica della decorrenza dei termini di prescrizione ovvero di decadenza: a seconda se il periodo di circolazione e mantenimento dei dati sia considerato rilevante o meno da un punto di vista giuridico, logicamente questo tempo dovrebbe esser computato per la decorrenza dei termini suddetti ovvero non tenuto in considerazione.

Si ritrova un'incidenza anche per il profilo soggettivo: oltre ai già citati problemi dell'anonimato e della c.d. <<vittimizzazione collettiva>>[749], bisogna chiedersi fino a che limite può essere attribuita una responsabilità a titolo di colpa o dolo alla <<sottostante "volontà" dei soggetti umani>>[750] relativamente quei contenuti avviati automaticamente dai sistemi e dai programmi- programmi che tuttavia loro stessi hanno avviato.

Infine, considerata l'entità dei danni percepiti dalle vittime in seguito la permanenza del contenuto illecito in rete (specie il c.d. <<danno sociale>>[751]), si è lamentato come le

[746]Picotti, *op.ult. cit*., pag. 93.
[747]Panattoni*, I riflessi penali del perdurare nel tempo dei contenuti illeciti nel Cyberspace*, in *Sistema Penale*, 2020, vol.5, pag. 305.
[748]Panattoni, *op. cit*., in pag. 318 e ss., esegue un quadro accurato delle diverse prospettive. L'orientamento maggioritario sarebbe nel considerare la consumazione del reato solo quando il contenuto viene posto online- conseguentemente, la permanenza del contenuto online non avrebbe alcuna rilevanza penale, in quanto solo <<manifestazione delle sole conseguenze del reato>> (pag. 319). Tra le diverse teorie prospettive enunciate, vi sono però altri autori (come Picotti, *op. cit.,* pagg.91-92) che invece sottolineano che bisognerebbe eseguire una distinzione tra la fase iniziale di <<perfezione formale>> e quella successiva di <<consumazione sostanziale>>.
[749]Si fa diretto richiamo al profilo degli autori e delle vittime dei reati cibernetici trattato nel punto 1.3. di questo capitolo.
[750]Picotti, *op. cit*., pag. 90.
[751]Come indicato da: Lavorgna, *Guardando oltre la criminalità informatica: l'importanza dell'approccio criminologico del "danno sociale" per osservare il ciberspazio con sguardo critico*, in *Ciberspazio e Diritto*, 1-2022, vol. 22, n. 67, pag.43; il danno sociale corrisponderebbe alla <<negatività emotiva o materiale, o al mancato soddisfacimento di un bisogno individuale>>, ed in esso sono compresi i danni fisici, finanziari, economici, emotivi,psicologici e culturali, percepiti direttamente (o indirettamente) dalle vittime.

sanzioni previste per i reati cibernetici ed informatici non siano in grado d'adempiere pienamente alle loro finalità riparatorie[752].

Vi è però un altro elemento, rilevante sotto il profilo penale,particolarmente messo in crisi dalle dinamiche del mondo cibernetico, già accennato nei paragrafi precedenti: lo spazio. Se la sfera cibernetica è costituita dalle innumerevoli relazioni che si creano, modificano e si cancellano senza sosta, è opportuno soffermarsi sul se e sul come essa abbia influenzato la nozione giuridica di "luogo" nel diritto penale.

3.1. Il principio di territorialità ex art. 6 c.p.: come si applica nel cyberspazio?

Quest'argomento è riassumibile come <<lo scontro tra il mondo reale ed il mondo virtuale>>[753]: il contrasto tra il concetto di spazio cui fa riferimento il diritto penale <<tradizionale>> e quello che viene definito come <<luogo informatico>>è talmente evidente da render necessaria una trattazione a parte.

Bisogna però procedere con ordine, portando come prima cosa all'attenzione le nozioni che si ritrovano nel sistema penale relative al luogo di commissione del reato nell'ordinamentogiuridico nazionale: non si può dunque non menzionare i principi indicati nell'articolo 3, comma 1°,e nell'articolo 6, comma 1°,del Codice Penale: il principio d'obbligatorietà della legge penale[754], secondo cui la norma penale vincola chiunque si trovi sul territorio nazionale; ed il principio di territorialità, secondo cui il diritto penale italiano s'applica in tutto il territorio nazionale, <<in connessione con sovranità ed indipendenza statale>>[755].

---

[752] Picotti, *Intercettazioni "illegali" tra nuove tecnologie e vecchi strumenti penali*, in *Dir. Int*., 2007, vol.2, pagg. 117-119.

[753] Seminara, *Locus commissidelicti, giurisdizione e competenza nel cyberspazio*, relazione al Convegno "Presi nella rete - Analisi e contrasto della criminalità informatica", Pavia, 23 novembre 2012, consultato in data 04/06/2023 in www.flamminiiminutochiocci.it/public/pubblicazioni/Giurisdizione_italiana_per_diffamazione_internet_dall_es.

[754]Si riporta qui le disposizioni, rispettivamente, dell'art. 3^1 c.p.: << La legge penale italiana obbliga tutti coloro che, cittadini o stranieri, si trovano nel territorio dello Stato, salve le eccezioni stabilite dal diritto pubblico interno o dal diritto internazionale>>; nonché l'art. 6^1 c.p.:<<Chiunque commette un reato nel territorio dello Stato è punitosecondo la legge italiana >>.

[755] Flor, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in Cadoppi,Canestrari, Manna, Papa, *Cybercrime,*2019, UTET Giuridica, pag. 144.

Pur essendovi dei limiti a questi principi[756], è sufficiente menzionare in questa sede il riferimento al diritto internazionale ex art. 3 c.p.: in estrema sintesi, lo Stato Italiano può sottoporre a processo penale lo straniero solo se vi è <<un collegamento con lo Stato del giudice>>[757], nonché sempre nel rispetto dei diritti e delle tutele per l'uomo.

Bisogna poi menzionare[758] che, al fine dell'individuazione del *locus commissidelicti*, vi è l'accoglimento del criterio dell'ubiquità: seppur in dottrina ed in giurisprudenza vi siano ancora dei dibattiti sulla sua applicabilità per il tentativo ex art. 56 c.p.[759], sembra esser predominante l'adozione del criterio in questione, secondo cui il reato è considerato commesso nel territorio statale <<quando anche solo una parte di esso [….] sia avvenuta sul territorio nazionale>>[760], purché, in base ad una valutazione *ex post*, quella stessa parte sia stata essenziale per la configurazione del reato stesso.

A questi elementi cardine del sistema penale tradizionale si contrappone la definizione di <<luogo informatico>>, i cui tratti peculiari sono oggetto anche adesso di studio e di dibattiti. Si è rilevato, in proposito, che emerge un conflitto vero e proprio tra due aspetti: l'astratta dimensione fisica in cui si trovano tutte le informazioni <<utilizzate direttamente dall'utente o da questi trasmesse in via telematica>>[761], e <<la partecipazione dell'utente>>[762], con la quale, tramite l'uso degli strumenti informatici, il soggetto contribuisce a creare questo spazio virtuale che utilizza.

Questi due elementi summenzionati sono stati utilizzati in due diverse prospettive dalla dottrina e dalla giurisprudenza per la risoluzione della problematica dell'inquadramento giuridico di questa nuova nozione di luogo informatico. Andando più nel dettaglio, si dovrà esaminare la <<prospettiva oggettivista>> e la <<prospettiva soggettivista>>.

La <<prospettiva oggettivista>> o <<patrimonialista>> predilige collegare la nozione di luogo informatico a quella di una cosa: conseguentemente, il dato informatico sarebbe

---

[756]Si fa espresso richiamo agli artt. 7-8-9-10 C.P.

[757] Flor, *op. cit.,* pag.145.

[758]Art. 6[2]c.p. :<<Il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione.>>

[759]Foggetti, *Il superamento del principio di territorialità: quale diritto applicare ad Internet,* in *Ciberspazio e Diritto*, 2004,Vol.5, n.3, pag. 233; v. pure Fiandaca, Leinieri, *Sub art. 6 c.p.*, cit., in Forti, Seminara, Zuccalà, *Commentario breve al codice penale*, 2017, CEDAM, pag. 37 e ss.Per la giurisprudenza: Cass. pen. Sez. III, del 10/05/1961, in *Cass. pen*., 1961, vol.II, pag. 811; Cass. sez. IV, 22/2/1993, in *Riv. Pen*. 1993, pag. 416.

[760]Foggetti, *op. cit.*, pag. 234. Nello stesso senso: Flor, *op. cit.,* pag. 146, il quale aggiunge, alla stessa pag., per completezza al discorso, anche la disamina degli artt. 8-9 c.p.p., in base ai quali si determinano i criteri di competenza del giudice penale italiano.

[761]Scuderi, *Un caso di hacking: luoghi reali e luoghi virtuali tra diritto e informatica,* in *Ciberspazio e diritto*, 2006, Vol.7, n.3, pag. 387

[762]*Ivi*, pag. 388.

riconducibile alle categorie delle <<*res corporales*>> ovvero <<*res incorporales*>>[763]<<piuttosto che ad un *tertium genus* autonomamente configurabile>>[764]. La dottrina a sostegno di quest'ipotesi fa riferimento alla concezione formalistica[765] dei beni intesi in senso giuridico ex art. 810 c.c.[766]: considerato che, secondo la stessa, i beni sono tali in quanto in grado di soddisfare i bisogni e gli interessi, si deve desumere che anche Internet sia un bene in senso giuridico, potendo dunque quasi assimilare il luogo informatico come bene all'interno del patrimonio.

Anche la giurisprudenza a sostegno della posizione ha evidenziato in particolare l'<<allargamento della nozione tradizionale di domicilio da quello fisico>>[767], in modo da tutelare gli utenti da un eventuale accesso abusivo[768]. Per il raggiungimento di questo fine, la giurisprudenza tende a non considerare l'aspetto <<fisico>> del domicilio, poiché in questo caso lo <<spazio virtuale>> altro non corrisponde se non metaforicamente al domicilio reale stesso: di conseguenza, anch'esso è meritevole d'apposita tutela giuridica.

A questa prima impostazione si contrappone << la prospettiva soggettivista>>, incentrata nel vedere il luogo informatico come espressione della personalità del soggetto e della sua creatività. Questa prospettiva è stata utilizzata in dottrina ed in giurisprudenza a sostegno della tutela del diritto d'autore in rete, nonché per l'esigenza di garantire misure di sicurezza per la riservatezza dei dati informatici.[769]

Senza soffermarsi molto sulle critiche rivolte alle prospettive presentate, l'aspetto interessante che si vuol far coglierè la concreta difficoltà d'inquadramento giuridico del luogo informatico, dovuta a due fattori principali: la difficoltà d'individuazione di una linea netta di demarcazione tra <<una dimensione oggettiva e una dimensione

---

[763]Senza soffermarsi molto sulla distinzione, si fa riferimento a due diverse categorie del Diritto Romano: citando Baldessarelli, *A proposito della rilevanza giuridica della distinzione tra 'res corporales' e 'res incorporales' nel diritto romano classico*, in *RIDA,* Vol.XXXVII, 1990, a pag.74,le *res corporales* sono quelle cose che possono esser percepite coi nostri sensi, mentre le *res incorporales*<<sono diritti e situazioni giuridiche, perché possono percepirsi con il solo intelletto>>.

[764]Scuderi*, op. cit.*, pag. 394.

[765]A sostegno di questa tesi si ritrova:Trabucchi, *Manuale di Diritto Civile*, 47esima edizione, CEDAM, 2015,pag. 613 (<<[…] il concetto di bene coincide pertanto con una qualificazione giuridica di ciò che può formare oggetto d'interesse umano>>); Torrente-Schelsinger, *Manuale di Diritto Privato*, 1995, Giuffrè, pag. 108.

[766]Riportando la disposizione dell'articolo in questione:<<Sono beni le cose che possono formare oggetto di diritti.>>

[767]Scudieri, *op. cit*., pag. 401.

[768] Si fa riferimento a: Cass. Pen.,Sez. V, n.12732/2000, cit., in *Cass. Pen.*, 2002, pag. 1015. Cfr. anche: Cass. Pen., Sez. VI del 4/10/1999, in *Foro It.,*2000,Vol. 123, n.3, pagg. 133-140.

[769]Scudieri*, op. cit.,* pag. 411, fa riferimento a: Trib. Torino, n. 753/2004, cit., in *Guida al Diritto,* 2004, pag. 65.

soggettiva>>[770] delle informazioni digitali che circolano nel cyberspazio; poi anche il fatto che il cyberspazio non può esser collocato definitivamente in una categoria giuridica preesistente, perché la sua nascita e il suo sviluppo sono intrinsecamente legati alla figura dell'utente (sia per l'uso individuale che ne fa, sia per <<l'interconnessione telematica>>[771], con cui si realizza il calcolo e la trasmissione dei dati stessi).

Sulla base di quanto detto finora, si può dunque notare come il persistente intreccio di creazione, modifica ed eliminazione delle relazioni nel Cyberspazio abbia trasformato il concetto di spazio, che in questo contesto assume una <<struttura bipartita>>[772]: esso può divenire soggetto o oggetto a seconda delle circostanze presenti e degli interessi in gioco.

In base a quanto detto, è chiaro che lo stretto principio di territorialità ed il criterio di ubiquità accolti nel diritto penale italiano fanno fatica ad applicarsi rispetto alla nuova dimensione cibernetica – se non addirittura rischia di esserci un problema di assoluta incompatibilità.
Di questo il giudice italiano si è reso conto giàall'inizio degli anni 2000[773]: vista l'esigenza europea di creare sul fronte della giurisdizione delle corti nazionali uno spazio europeo collaborativo ed in grado di estendersi al di fuori dei propri territori nazionali, s'individuò negli artt. 3 e 11 della Costituzione Italianaelementi sufficienti per far sì che il diritto comunitario rientrasse nel limite penale del principio di territorialità ex art. 3 c.p., consentendo dunque <<un superamento del principio di stretta territorialità nei casi di criminalità informatica transnazionale>>[774].

Peraltro, se non fosse avvenuto questo passaggio, l'Italia avrebbe dovuto comunque superare questo ostacolo, perché nella Convenzione di Budapest (che, si ricorda, l'Italia ha ratificato con la l. 48/2008[775]) si rileva che la competenza deve strutturarsi sul principio di

[770]Scudieri, *op. cit*.,pag. 414.
[771]*Ivi*,pag. 420
[772]*Ivi*,pag. 415.
[773]Si fa riferimento a Trib. Milano, 1/3/2001, in *Riv. It. dir. e proc. Pen.,* 2002, fasc. 1, pag. 367, dove, riguardo al limite della legge internazionale individuato all'art. 3^1 c.p., << […] Sebbene tale importante limite sia stato sempre interpretato quale clausola di salvaguardia dell'applicabilità soggettiva della legge penale (pensando soprattutto alle immunità), non può negarsi che la norma "de qua" si presta fisiologicamente e automaticamente a recepire nuovi confini della legge penale in relazione all'evoluzione del diritto pubblico interno e del diritto internazionale>>.
Per maggiori approfondimenti su questa sentenza, si cita: Mazzini, *Prevalenza del diritto comunitario e non obbligatorietà della legge penale: un rapporto interessante, ma non sostenibile*, in *Rivista italiana di diritto e procedura penale,* 2002, fasc. 1, pag. 368-380.
[774]Foggetti, *op. cit.,* pag. 238.
[775]SI fa richiamo al paragrafo 2.2.

territorialità[776], ma <<se il reatonon sia punibile nel luogo in cui è stato commesso ovvero non rientri nella competenza territoriale di nessuno Stato>>[777],dovrebbe invece trovare applicazioneil principio della personalità attiva[778].
Bisogna aggiungere però che non tutti gli Stati aderenti alla Convenzione riconoscano ai medesimi livelli i principi summenzionati: se la personalità attiva è un principio che in alcuni Stati ha un massimo riconoscimento (ad es., all'interno del codice penale tedesco), in altri invece vi è una considerazione di esso ridotta solo agli aspetti essenziali (come quello italiano)[779].

Oltre a ciò, si è ben consapevoli che non sia per nulla semplice applicare uniformemente questi principi ad una materia così sfuggente e ancora indecifrabile come quella del cybercrime: è importante chiarire che - ancor prima delle problematiche relative alla giurisdizione e competenza che sono sorte sia a livello nazionale che sovranazionale[780]- quest'espansione del tempo e dello spazio creata dalla caratteristica dell'automazione (e dalla successiva circolazione e mantenimento in rete dei dati) rende molto complessa l'individuazione del momento e del luogo diconsumazione del reato, tanto da dover necessariamente affrontare la problematica caso per caso[781].

[776]Per completezza, si riporta qui la disposizione dell'art. 22[1-2] della Convenzione: <<Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per stabilire la propria competenza per tutti i reati previsti in conformità agli articoli da 2 a 11 della presente Convenzione, quando i reati siano commessi:
a.. nel proprio territorio;
b. a bordo di una nave battente bandiera della Parte;
c. a bordo di un aeromobile immatricolato presso quella Parte;
d. da un proprio cittadino, se l'infrazione è penalmente punibile là dove è stata commessa o se l'infrazione non rientra nella competenza territoriale di alcuno Stato.
Ogni Parte può riservarsi il diritto di non applicare o di applicare solo in condizioni o casi specifici le regole di competenza dettate dai paragrafi 1.b – 1.d del presente articolo o in una parte qualunque di essi.>>
[777]Seminara, *op. cit*., pag. 6. Nello stesso senso: Flor, *op. cit*., pag. 150.
[778]Il criterio della personalità attiva, secondo il quale ad ogni autore di reato si applica la legge dello Stato cui egli appartiene,è uno dei principi (assieme a quello dell'universalità e della personalità passiva) con cui viene mitigato il criterio di territorialità ex art. 6 c.p., Sulla base di esso, lo Stato può applicare la propria legge ai cittadini che commettono reati all'estero, ma allo stesso tempo non si possono punire gli stranieri che commettono reati sul territorio nazionale se il fatto non è previsto come reato dalla legge dello Stato di appartenenza.
[779]Seminara, *op. cit*., pagg. 6-7.
[780]Seppur non si tratterà oltre dell'argomento perché rientrante nella parte processuale penale, per ulteriori approfondimenti si fa richiamo a:Flor,*I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, (nota a Cass. Sez. Un., n.17325/2015), in *Dir. Pen. Proc*., 2015, n.10, pagg.1296-1310.
[781]Flor, *op. cit*., pag. 153.

Inoltre, sulla base di un'attenta analisi eseguita su un caso di diffamazione avvenuto nel 2000[782], emergono degli interrogativi sul principio di territorialità e di personalità attiva che potrebbero esser considerati anche di carattere generale.

Anzitutto, considerando la capacità dei mezzi cibernetici, informatici e telematici di superare i confini nazionali, risulta piuttosto ardua<<l'individuazione del luogo in cui deve ritenersi consumato il delitto commesso "a mezzo Internet">>[783].

Inoltre,secondo il principio di territorialità ex art. 3 c.p.[784], si dovrebbe punire secondo il diritto penale italiano il soggetto che si ritrovi fisicamente sul territorio statale: e se, ad esempio, il soggetto non fosse in Italia, ma utilizzasse programmi informatici ovvero macchine informatiche o telematiche prodotte in Italia[785]? Varrebbe comunque questo principio?

Data la natura transnazionale dei crimini cibernetici, per risolvere queste problematiche è dunque necessario un intervento normativo sul pianointernazionale che affronti direttamente queste tematiche, al fine di fronteggiare <<l'anarchia di Internet e l'anarchia del diritto>>[786]; si riafferma inoltre la necessità di un intervento legislativo nazionale più attento alle caratteristiche del ciberspazio, soprattutto in ambiti (come quello dell'individuazione del luogo di reato) <<maggiormente a rischio di forzature e distorsioni interpretative>>[787].

[782]Si fa riferimento ad un caso di diffamazione tramite social media e network in Cass. pen.,Sez. V , n. 4741/2000, in http://www.interlex.it/testi/cp4741.htm. Per maggiori approfondimenti sulle riflessioni eseguite sulla motivazione e le argomentazioni della sentenza, si rinvia direttamente a: Flor, *op. cit*., pagg.155-157; Seminara, *(voce) Internet, in Enciclopedia del diritto. Annali*, vol.7, 2014, Giuffrè, pag.. 577 e ss. .

[783]Foggetti, *op .cit*., pag. 234.

[784]<<La legge penale italiana obbliga tutti coloro che, cittadini o stranieri, si trovano nel territorio dello Stato>>.

[785]Nella specificità della controversia, si faceva riferimento al <<soggetto che gestisce quotidianamente […] degli account regolarmente registrati dei sistemi informatici italiani>>

[786]Seminara, *op. cit.* ,pag. 14.

[787]Flor, *op. cit*., pag. 157.

Capitolo III: L'associazione a delinquere online

Nel primo capitolo si sono trattate le principali critiche mosse alla fattispecie di cui all'art. 416 c.p., e si è visto poi nel secondo capitolo come la dimensione cibernetica abbia letteralmente sconvolto ogni aspetto della vita umana,incluso l'ambito criminale, considerando come in esso vi sia stato un aumento esponenziale della varietà e tipologie di reati commessi (sia preesistenti che nuovi).

In questa fase finale di questo lavoro si cercherà d'unire i due discorsi indagando come le associazioni a delinquere si comportano nella realtà cibernetica, sulla base degli attuali studi della dottrina e delle più recenti pronunce della giurisprudenza.Oltre al fatto che questo è un campo recente, su cui ancora non vi è un orientamento giurisprudenziale consolidato ed una frammentaria visione negli studi dottrinali, ci sono due importanti premesseda fare prima di addentrarsi nella trattazione dell'argomento.

La prima è capire in che luogo operano queste associazioni a delinquere: viste le difficoltà d'inquadramento delle diverse tipologie di reato anche rispetto allo spazio, è doveroso fare una breve parentesi nel comprendere meglio la struttura di Internet.

Questo perché - come si vedrà a breve – seppur i reati cibernetici siano presenti in qualsiasi angolo della rete, vi è un sostrato non immediatamente accessibile agli utenti, ma in cui avvengono la stragrande maggioranza attività criminali in Rete, organizzazioni illecite comprese. Bisogna dunque distinguere tre <<livelli>> nella rete Internet.

Lo strato più superficiale è quello del c.d. <<Clear Web>> [788], caratterizzato dalla rintracciabilità: ad ogni singolo individuo che naviga in questa rete viene associato un indirizzo IP[789] non appena si collega in essa, in modo da poter facilmente identificare quale sia il dispositivo connesso in Internet. È la <<parte>> più conosciuta ed utilizzata dalla popolazione mondiale, ma è da sottolineare che è una parte piccolissima della Rete: essa equivale al 4% dei dati e delle informazioni che la costituiscono[790];

---

[788]Massa, *Il deep web ed il dark web,* in AA.VV., *Diritto di Internet. I crimini informatici, il dark web e le web room (vol. II),* (a cura di) Bassoli, Pacini Editore, 2021, pag. 38.

[789]Come indicato da: Massa, *op. cit.,*pag. 39, l'Indirizzo IP (Internet Protocol) è una serie di quattro numeri intervallati da punto che permette di identificare l'utente quando naviga in rete. Nella stessa pagina viene richiamata la sentenza Cass. pen. Sez. V., n. 20485/18, in*Guida al diritto,*2018, N..26, pag.80 ,secondo la quale l'IP corrisponde a <<il dispositivo elettronico associato>>, tuttavia l'identificazione dell'utente a fini processuali richiede ulteriori indagini. Si cita anche: Pascuzzi, *op.cit*., pagg. 55-59.

[790]Massa, *op. cit.,* pag. 40. Almomani, *Darknet traffic analysis, and classification system based on modified stacking ensemble learning algorithms,* in *Information Systems and e-Business Management,*2023, (DOI: https://doi.org/10.1007/s10257-023-00626-2) riferisce invece che i motori di ricerca del Clear Web più utilizzati (es. Google, Yahoo, etc.) forniscono dati ed informazioni, nonché indirizzano a contenuti corrispondenti al 5% di quanto è presente in Internet.

Il sostrato restante di Internet è costituito dal c.d. <<Deep Web>>[791]. Nato durante il periodo della Guerra Fredda per lo scambio di informazioni scientifiche ad uso militare, oggi è una dimensione sommersa enorme, dove si ritrova la quasi totalità del materiale contenutistico presente in rete. Caratteristica essenziale – a differenza del Clear Web- è l'assenza di indicizzazione dai motori di ricerca: in esso è garantito l'accesso solo a soggetti dotati di particolari doti informatiche e aventi particolari software a disposizione che permettano di poter navigare in anonimato, senza che avvenga la registrazione automatica dell'indirizzo IP (il più noto di essi è il c.d.<<Browser TOR >>[792]).
Spesso il Deep Web nell'immaginario collettivo viene percepito come la parte illecita del Web: questa accezione non è del tutto corretta[793], poiché esso è anche un luogo in cui si possono esprimere i propri pensieri e diffondere informazioni in totale libertà (ad es. informazioni politiche o militari riguardanti regimi dittatoriali in cui si vive), nonché in esso vi è un mercato in cui si possono anche acquistare legalmente beni di difficile reperibilità[794].

Tuttavia, vi è nel Web sommerso una piccola parte in cui si accede a contenuto esclusivamente illecito:si parla infatti del c.d. <<Dark Web>>[795], il livello di maggior difficoltà d'accesso: oltre ai requisiti indicati nel Deep Web, sono infatti necessarie ulteriori capacità informatiche e conoscenze tecniche da parte dell'utente per non solo accedervi, ma anche per saper adeguatamente navigare in esso.
È in questo <<sottoinsieme del "Deep Web">> [796] che avvengono la stragrande maggioranza delle attività illecite[797], proprio per la difficoltà di tracciamento e l'anonimato garantito da questa parte di Internet ad ogni utente[798].

---

[791]Massa, *op. cit.,* pag. 37, definisce il Deep Web come <<quella parte del Web in cui risiedono pagine indicizzate dai motori di ricerca>> (es. Google, Microsoft Edge, Mozilla Firefox, Yahoo, etc.).
[792]Il Browser TOR (*The Onion Router*) è un software legale, che inserisce dei soggetti intermedi (chiamati <<nodi>>) tra l'utente e la pagina finale, creando un vero e proprio <<sistema a cipolla>>: in questo modo, considerando che questa linea di <<nodi>> cambia di volta in volta, si consente agli utilizzatori del software la massima sicurezza nel navigare in rete e l'anonimato. Si cita: Massa, *op.cit*., pag. 41; Di Corinto*, Che cos'è il Tor project e a cosa serve*, pubblicato il La Repubblica.it il 3/11/2017.
https://www.repubblica.it/tecnologia/sicurezza/2017/11/03/news/che_cos_e_tor_e_a_che_cosa_serve-180152431/ .
[793]Si veda, al tal proposito:Di Corinto, *Tutti i Segreti del Deep Web*, pubblicato in La Repubblica.it il 20/04/2014.
https://www.repubblica.it/tecnologia/2014/04/20/news/tutti_i_segreti_del_deep_web-84053410/.
[794]Massa, *op. cit.,* pag. 44.
[795]Per maggiori approfondimenti sulla struttura del Dark Web, si richiama direttamente a: Rajawat, Bedi, Goyal, Kautish, Xihua, Aljuaid,Mohamed*, Dark Web Data Classification Using Neural NetworkComputational intelligence and neuroscience*, 2022, 8393318. (DOI: https://doi.org/10.1155/2022/8393318)
[796]Massa, *op. cit.,* pag. 61.

Qui si trova un vero e proprio mercato illecito (ad es., tra i beni in commercio, si possono reperire: materiale contraffatto, sostanze stupefacenti, ma anche turismo sessuale e/o materiale pedopornografico, programmi o software per l'inserimento di virus e/o malware da utilizzare contro destinatari specifici, offerte di ingaggio per lesioni personali e/o omicidioverso qualcuno[799]).

Ma non solo: si trovano in essi dei servizi che si potrebbero definire come un <<riflesso in versione illegale>> rispetto ai servizi che si trovano nel Clear Web: ad es.<<Hidden Wiki>>[800], i c.d. <<social dark>>[801], nonchéforum e <<chatroom>>dove chiunque può discutere di qualunque argomento, sia lecito che illecito.

Sarà proprio su queste ultime che si focalizzerà l'attenzione, poiché è proprio in esse dove (come si vedrà a breve) frequentemente si creano le basi delle associazioni a delinquere operanti online.

La seconda premessa necessaria è incentrata sul fatto che i gruppi criminali organizzati operanti online sono diventati un fenomeno di studio sul profilopenalistico in un'apposita categoria socio-criminologica, il c.d. <<cyber organized crime>>[802]: nata dall'unione delle

---

[797] Si vuol far notare che si parla di <<stragrande maggioranza>>, non di totalità: come si è indicato precedentemente, i reati cibernetici ed informatici si consumano in ogni angolo della Rete, compresa quella <<visibile>> - ad es., si segnala la tendenza dell'utilizzo dei social network (es. Facebook, Whatsapp, Telegram) per lo scambio di materiale e contenuto illecito(es.droga, contenuti di carattere pornografico, dati sensibili rubati, carte di credito, ecc.) nonché per un'intensa attività di propaganda e di reclutamento a scopi terroristici. Per maggiori approfondimenti sul punto, si richiama direttamente a: Cosimi, *Altro che Deep Web, il cyber crimine è di casa sui social network*, pubblicato in La Repubblica.it il 28/09/2016. https://www.repubblica.it/tecnologia/sicurezza/2016/09/28/news/cybercrimine_altro_che_deep_web_sui_social_network_e_di_casa-148645562/; Neto, *Social Network Analysis and Organised Crime Investigation: Adequacy to Networks, Organised Cybercrime, Portuguese Framework*, in *Cybercrime, Organized Crime, and Societal Responses International Approaches*, Viano, Springer International Publishing AG, pagg. 179 e ss. (DOI: https://doi.org/10.1007/978-3-319-44501-4); Lamberti, *op. cit.,* pag. 140.

[798] Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing,* in *Global Commission on Internet Governance Paper Series,* 2017, N°21, pagg.39-42.(DOI: http://dx.doi.org/10.2139/ssrn.2667711).

[799] Massa, *op. cit.,*pagg. 48-49; ma sivedaanche: Spagnoletti, Ceci, Bygstad, *Online Black-Markets: An Investigation of a Digital Infrastructure in the Dark*, in *Information Systems Frontiers*, 2022, Vol. 24, Is. 6,pagg. 1811-1826. (DOI:https://doi.org/10.1007/s10796-021-10187-9); Zaami, *New Psychoactive Substances and evolving criminal dynamics against the backdrop of the fourth industrial devolution, in* Acta Biomed, 2022; Vol. 93, N. 2. DOI: 10.23750/abm.v93i2.13008.

[800] Massa, *op. cit.,* descrive a pag. 51<<Hidden Wiki>> come un'enciclopedia posta sul modello di Wikipedia, dove si trova una completa catalogazione delle pagine web e dei servizi che si ritrovano sul Dark Web <<per genere e contenuto secondo delle regole precise e ferree in merito all'aggiornamento, all'aggiunta e alla gestione degli indirizzi oltre che alla descrizione dei contenuti che vi sono al suo interno>>.

[801] Massa, *op. cit.,*definisce a pag. 52 i <<dark social>> come la versione in anonimato e sul DeepWeb dei social network presenti nel Clear Web: come alcuni esempi viene citato <<Dark Facebook>> (anch'esso sviluppato sul modello di Facebook), nonché <<Black Box>>, <<espressamente progettato per agire nel Dark Web>> e dove si crea un nuovo profilo anonimo per accedere ad esso.

Per maggioriapprofondimentisulpunto, sirichiama: Burcher, Whelan, *Social network analysis as a tool for criminal intelligence: understanding its potential from the perspectives of intelligence analysts*, in Trends in Organized Crime, 2018, Vol.21, Is.3, pagg. 278-294. (DOI: https://doi.org/10.1007/s12117-017-9313-8).

[802] Di Nicola, *Towards digital organized crime and digital sociology of organized crime,* in *Trends in Organized Crime*, 2022 (DOI: https://doi.org/10.1007/s12117-022-09457-y).

categorie del cybercrime e della criminalità organizzata, essa viene definita come<<sia la criminalità organizzata tradizionale che ha spostato alcune sue attività illecite su internet, sia i comuni cyber criminali che agiscono in maniera organizzata sul web>>[803] .

Da questa nozione si ricava il fatto che vi sono multiple forme di associazioni a delinquere operanti online e con caratteristiche diverse tra loro. Gli studiosi[804] le hanno distinte in due macrocategorie.

Le prime sono le c.d. associazioni per delinquere <<esclusivamente cibernetiche>>, organizzazioni aventi come obiettivo l'esclusiva commissione di reati cibernetici. In questo caso, tutti gli elementi del fatto tipico ex art. 416 c.p. saranno esistenti solamente nella dimensione cibernetica. In questa categoria rientrano: le associazioni a delinquere dedite allo scambio di materiale pedopornografico, i gruppi di <<hacktivisti>> [805] e le organizzazioni gestenti i mercati/forum illegali online.

Tutt'altra cosa sono invece le <<associazioni per delinquere cibernetiche ibride>>, organizzazioni criminali finalizzate *sia* alla commissione di reati cibernetici, *sia* alla commissione di <<reati tradizionali>>nella realtà fisica. A differenza delle prime, solo il programma criminoso ha caratteristiche virtuali, mentre l'organizzazione è presente nella dimensione fisica. Elencando alcuni esempi di questa categoria, vi sono: le organizzazioni dedite alle truffe online[806], le organizzazioni dedite al mercato illegale dello streaming e le mafie tradizionali inserite nel business del gioco d'azzardo online[807].

---

[803] McCusker, *Transnational organised cyber crime: distinguishing threat from reality*, cit., in *Crime Law and Social Change*, 2006, vol. 46, pag. 258. DOI: 10.1007/s10611-007-9059-3.

[804] Si fa riferimento a: Grabosky, *The Internet, Technology, and Organized Crime*, in *Asian Journal of Criminology* 2007, Vol. 2, pag. 154-155. DOI : 10.1007/s11417-007-9034-z . Di Nicola, *Towards digital organized crime and digital sociology of organized crime*, in *Trends of Organized Crime,* 2022 (DOI: https://doi.org/10.1007/s12117-022-09457-y). *Contra:*McGuire, *Organised crime in the digitalage*, cit. , John Grieve Centre for Policing and Security and BAE Systems Detica,2012, (http://www.baesystemsdetica.com/uploads/resources/ORGANISED_CRIME_IN_THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf), secondo cui vi sarebbero tre le tipologie:oltre a quelle esclusivamente virtuali e ibride, vi sono anche quelle organizzazioni che agiscono prevalentemente offline, ma che utilizzano le tecnologie cibernetiche ed informatiche per agevolare le loro attività.Cfr. anche: Lavorgna, *Cyber-organised crime. A case of moral panic?,* in *Trends in Organized Crime* , 2019, Volume 22, Issue 4, pagg.357–374 (DOI: https://doi.org/10.1007/s12117-018-9342-y/), secondo cui, a pag. 370,la catalogazione delle tipologie di cybercrime e i rispettivi collegamenti alla criminalità organizzata non sono affatto da sottovalutare: dal numero di essi dipende non solo l'entità dell'azione repressiva svolta dagli Stati contro queste tipologie di reati, ma anche il livello di ansia e di terrore generale che si può diffondere nella popolazione.

[805] Le comunità online di pedopornografia e gli <<hacktivisti>> verranno trattati più in dettaglio nel punto 1.3. e nel paragrafo 2 di questo capitolo.

[806] Un classico esempio sono le organizzazioni criminali dedite alla commissione del già menzionato reato del phishing. Riprendendo le parole di De Vivo, Ricci, *op. cit*., pagg. 56-57 , il phishing è <<una frode informatica che, attraverso il furto di identità, induce gli utenti a rivelare informazioni e codici riservati e con essi si compiono illeciti come prelievi bancari e ricariche telefoniche>>. Una volta ottenuto il denaro, vi sono altri membri dell'organizzazione che procedono sia alla rivendita dei dati bancari nel mercato nero illecito del Dark Web, nonché ad eliminare ogni traccia sul server della vittima. Per maggiori approfondimenti sul punto, si fa riferimento a: Tehrani,Kavon, Pontell. *Phishing Evolves: Analyzing the*

Per la vastità degli argomenti, non è possibile approfondire entrambe le categorie in questa sede: si procederà alla sola trattazione delle associazioni a delinquere operanti esclusivamente online.

Nel prosieguo verrà dunque dato un profilo criminologico e giuridico generale su questo fenomeno, passando poi alla trattazione delle diverse modalità organizzative, per chiudere delineando in via approssimativa alcuni tratti caratteristici delle associazioni a delinquere aventi come oggetto del programma lo scambio di materiale pedopornografico: tutti elementi utili per affrontare poi l'associazione a delinquere di <<hacktivisti>> più famosa, ossial'associazione Anonymous.

1. Il profilo criminologico dei partecipanti all'associazione per delinquere online.

Per le medesime ragioni menzionate nel corso della disamina generale delle vittime e degli autori di reati cibernetici[808], è piuttosto arduo eseguire un criminal profiling del c.d. <<partecipante>> alle associazioni a delinquere online- non a caso spesso si esegue uno studio basato sulle specifiche tipologie di reato.

Nonostante la varietà delle associazioni a delinquere e dei loro programmi delittuosi – e, conseguentemente, delle ragioni che spingono gli individui a creare, aderire all'associazione e partecipare ad essa -, viene in soccorso il fatto che i soggetti coinvolti eseguono la loro condotta di partecipazione illecita esclusivamente *online*.

Un primo elemento che si può naturalmente dedurre è che si tratta spesso di individui che trascorrono online un quantitativo di tempo tendenzialmente maggiore rispetto ai partecipanti delle associazioni cibernetiche ibride (a volte arrivando anche a livelli di

---

Enduring Cybercrime, in *Victims & Offenders*, 2021, vol.16, n.3, pagg.316–342. DOI:10.1080/15564886.2020.1829224.

[807] Per maggioriapprofondimentisulpunto, si fa riferimento a: Lavorgna, *Organised crime goes online: realities and challenges*, in *Journal of Money Laundering Control*, 2015, Vol. 18, N. 2, pagg. 153-168. (DOI: https://doi.org/10.1108/JMLC-10-2014-0035); Choo, Smith, *Criminal Exploitation of Online Systems by Organised Crime Groups,* in *Asian Journal of Criminology*, 2008, vol. 3, n. 1, pagg. 37-60. (DOI: 10.1007/s11417-007-9035-y).

[808] Si fa un esplicito riferimento al Capitolo 2, paragrafo 1.4.

carattere patologico): di conseguenza, essi avranno una generale irreprensibilità di condotta nella vita di tutti i giorni[809], nonché elevate competenze di livello tecnico ed informatico.

Sulla base di alcune ricerche sulle motivazioni che spingono l'utente all'assunzione della condotta illecita di partecipazione ad associazioni dedite alla commissione dei reati cibernetici e/o informatici, risulterebbe esser predominante la motivazione di carattere economico[810].

Riguardo invece la loro personalità, aspetti comuni risultano essere:una certa ritrosia nel contatto sociale, la presenza di disturbi psicologici[811], la presenza di atteggiamento di superiorità basata sulla consapevolezza di difficoltà (se non impossibilità) di esser rintracciati[812], nonché l'estremizzazione del tratto del machiavellismo[813] a cui si possono aggiungere anche dei tratti di narcisismo patologico[814].

Altro punto da tenere in considerazione è che in rete l'utente di qualsiasi associazione a delinquere esclusivamente cibernetica ha l'obiettivo di non esser rintracciato in alcun modo: ragion per cui non solo i partecipanti sono utenti in anonimato ovvero utilizzanti avatar con informazioni pressoché false rispetto al quelle appartenenti alla propria persona

[809] De Vivo, Ricci, *op. cit.,* pag. 55, fanno riferimento a: Fedeli, Ricci, Cortucci, *Lineamenti di Criminologia*,cit., Edizioni Scientifiche Italiane, 2006, pag. 58 e ss.

[810]Broadhurst,Grabosky,Alazab,Chon, *Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime,* in *International Journal of Cyber Criminology,* 2014, Volume 8, Issue 1, pag. 3.

[811] Dalle analisi condotte da Niveau, *Cyber-pedocriminality: Characteristics of a sample of internet childpornographyoffenders*, in *Child Abuse&Neglection*, 2010, vol.34, Is.8, (DOI: 10.1016/j.chiabu.2010.01.01), a pag. 572 risulta che circa il 75% dei partecipanti testati risultavano avere dei disturbi della personalità. Nei casi più frequenti (circa il 58%) i soggetti mostravano, alternativamente o cumulativamente: una personalità di tipo dipendente (aventi dunque la concezione che gli altri siano gli unici a farli sentire bene e forti), ossessivo- compulsiva (la presenza di immagini, sensazioni o pensieri ricorrenti che inducono nell'individuo uno stato generale di ansia/disgusto, che lo porta a tenere dei comportamenti ripetitivi); nonché una personalità di tipo evitante (caratterizzata da un forte senso di inadeguatezza verso il prossimo, che può portare l'individuo ad un enorme timore del rifiuto o delle relazioni sociali, fino all'estrema emarginazione).

[812]Young,Zhang,Prybutok,*Hacking into the Minds of Hackers*, in *Information Systems Management,*2007, Vol. 24, n.4, pag. 286 (DOI: https://doi.org/10.1080/10580530701585823/)

[813] Riguardo il suo significato, si veda *supra* al Capitolo 2, paragrafo 1.4.

[814] Secondo: AA. VV., *Manuale Diagnostico e Statistico dei disturbi mentali*, 2014, Raffaello Cortina Editore, pag. 776, un tratto tipico del narcisismo patologico è la scarsa considerazione delle possibili conseguenze dei propri comportamenti rispetto alle vittime, il cui possibile danno è considerato insignificante rispetto al conseguimento dei propri obiettivi.

fisicareale[815], ma anchese ne trae che quasi nessun utente conosca effettivamente chi siano nella realtà gli altri membri[816].

Non si intende però andare oltre. Superati questi punti, le caratteristiche dei partecipanti divergono non poco, per tutta una serie di fattori. Elencandone alcuni: la moltitudine di associazioni a delinquere esclusivamente cibernetiche; la diversità delle modalità con cui il soggetto viene a conoscenza dell'esistenza di queste tipologie di associazioni a delinquere nel sistema cibernetico; l'abnorme numero delleragioni che spingono un membro ad aderire; la generale ritrosia dell'utente medio nel segnalare l'esistenza ovvero l'illiceità di queste associazioni a delinquere [817] - a prescindere se l'utente decida di divenire partecipante o meno.

1.1. L'hacker, il <<Robin Hood >> del Cyberspazio?

Al fine di dare sia maggior completezza a questo argomento, sia di fornire un'ulteriore prospettiva nella specifica trattazione delle associazioni a delinquere esclusivamente cibernetiche relativamente all'accesso abusivo e al danneggiamento di sistemi informatici, si passerà alla trattazione di una specifica figura di partecipante dell'associazione a delinquere online, il c.d. <<hacker>>[818]- forse la più nota nell'immaginario collettivo e

[815]Si richiama in questo proposito la <<dissociazione tra identità virtuale e digitale>> esplicata nel Capitolo 2, paragrafo 1.4. Ciò rende perciò molto arduo comprendere l'età predominante tra i partecipanti dell'associazione a delinquere online,i quali tendenzialmente sono di sesso maschile. Non a caso si parla delle <<identità ricostruite>> nello spazio cibernetico, proprio per la possibilità dell'utente di navigare in Rete con un'identità da poco a totalmente diversa (es. per genere, etnia, ecc.), creandosi quasi un vero e proprio <<personaggio>>. Questo è posto in evidenza da Papadimitriou, *A nexus of Cyber-Geography and Cyber-Psychology: Topos/''Notopia" and identity in hacking,* in *Computers in Human Behavior* 2009,vol.25, pag. 1333. (DOI:https://doi.org/10.1016/j.chiabu.2010.01.011/).

[816]Papadimitriou, *op.cit.*, pag. 1333. Cfr anche: Olson, *Noi siamo Anonymous*, (trad. Puggioni), 2013, Ed. Piemme, pag. 19.

[817]Le spiegazioni date a questo comportamento sono alcune tra quelle già elencate rispetto al profilo generale della vittima dei reati cibernetici affrontato nel Capitolo 2, paragrafo 1.4.: nello specifico, il << bilancio costi-guadagni>> ed una sfiducia nel sistema giudiziario e polizia. Si può aggiungere che, sulla base delle riflessioni svolte finora, una convincente ragione può esser pure un forte senso di inerzia e d'indifferenza dell'utente.

[818]L'hacker corrisponde al soggetto che esegue l'attività di <<hacking>> . Riportando la definizione data da Wikipedia (https://it.wikipedia.org/wiki/Hacking), l'attività di <<hacking>> deriva da*to hack (attaccare* , in inglese). Il termine comprende <<l'insieme dei metodi, delle tecniche e delle operazioni volte a conoscere, accedere e modificare un sistema informatico hardware (parte tangibile del computer, come, ad esempio il monitor, la tastiera o il mouse) o software (parte intangibile, traducibile come il supporto logico del computer)>>.

spesso caricaturata dai mass media[819], tanto da aver guadagnato l'appellativo de <<Il pirata del Web>>[820].

Nati originariamente come <<true hackers>> negli anni '60 - soggetti con particolari doti programmatiche, ingegneristiche ed informatiche che si sfidavano tra loro, ma seguendo comunque una certa etica[821], odiernamente si potrebbero approssimativamente definire come soggetti aventi delle abilità (più o meno elevate)per poter individuare eventuali punti deboli dei sistemi informatici o cibernetici e poterli sfruttare per i loro obiettivi.

Un dubbio che però sorge in primo luogo è se l'hacker possa davvero esser considerato davvero come un criminale, e – qualora la riposta precedente sia in senso affermativo- se possa divenire partecipante o meno di un'organizzazione criminale.

Partendo dalla prima domanda, non si può avere una risposta netta, considerando l'enorme numero di tipologie di hackerodiernamente esistenti. Sulla base di diversi parametri - un <<approccio <<interno>> (il livello di abilità e la loro sfera morale) che <<esterno>>(gli strumenti a loro disposizione ed il loro *modus operandi*) [822] , si possono ricavare alcune generali categorie.

I primi sono i <<White hats>> (che in un linguaggio semplicistico, si potrebbero definire come <<gli hacker buoni>>[823]). Sono hacker rispettosi della legge in tutto e per tutto: tendenzialmente si fermanonelle loro attività non appena vi sia qualunque potenziale azione illecita che possono commettere, poiché il loro obiettivo principale è quello di proteggere i computer, network e i sistemi da potenziali attacchi. Di elevate competenze tecniche, spesso lavorano da soli.

Seppur non particolarmente spinti dall'interesse economico, i <<cappelli bianchi>> possono esser ingaggiati da aziende private allo scopo di installare e controllare l'andamento dei loro sistemi di sicurezza in rete: in quel caso, il loro comportamento tende

[819]Ciuricina, *Etica Hacker?,* in *Digit Cult - Scientific Journal on Digital Cultures***,** [S.l.], 2020, volume 5, numero 1, pagg. 69-70, (DOI: https://doi.org/10.4399/97888255361647)
[820] Il titolo viene ripreso dal libro: Francione, *Hacker. I Robin Hood del Cyberspazio,* 2004,Lupetti.
[821] Jacquet-Chiffelle, Loi, *Ethical and Unethical Hacking*, in Christen, Gordijn, Loi, *The Ethics of Cybersecurity,*2020, Springer International Publishing AG (DOI: https://doi.org/10.1007/978-3-030-29053-5/), pag. 181, la definiscono come <<*hacker ethic* >> (da non confondere con *l'ethical hacking,* di cui si tratterà in seguito), consistente nel condividere liberamente le informazioni, un'antipatia per i poteri centralizzati e il desiderio di utilizzare i computer per costruire un futuro migliore.
[822]*Ivi*, pag. 188; Matulessy, Humaira, *Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits*, in Psychology and Behavioral Sciences, 2016, Vol. 5, n. 6, pagg. 138. (DOI: 10.11648/j.pbs.20160506.12).
[823] Si riprende l'espressione utilizzata da: Jacquet-Chiffelle,Loi, *op. cit.,* pag. 182.

ad essere ancora più rispettoso delle regole, allo scopo di guadagnarsi la fiducia dell'azienda stessa[824].

Vi sono poi i <<Grey hats>>: sono difficili da classificare, poiché a differenza dei << Black hats>> non hanno intenzioni malevole e non sono spinti dall'avidità, ma possono occasionalmente ignorare le regole se necessario per il raggiungimento dei propri obiettivi, e tentano di minimizzare il più possibile eventuali conseguenze dannose.Sono spesso dotati di elevate doti tecniche ed ingegneristiche ed agiscono di regola spinti da motivazioni legate al personale divertimento, ovvero per guadagnare rispetto tra gli altri utenti o per sfidarli in gare di abilità. Non risultano inoltre in alcun modo interessati a collaborare con le aziende.

Da ultimi, vi sono i c.d. <<*black hat*>>, soggetti che vengono inquadrati spesso tra i cybercriminali[825]: che sia per l'eccitazione che provano sul momento, o per guadagnarsi il rispetto tra gli altri hacker, per motivi economici o perché vista da loro come un'occasione di apprendimento, l'attività da loro svolta rientra indubbiamente nella sfera illegale, poiché puntualmente infrangeranno la legge per il raggiungimento dei propri scopi illeciti.
La loro scelta di violare ripetutamente la legge e di commettere atti illeciti è dovuta anche al disprezzo che nutrono per le autorità, non in grado di riconoscere ed apprezzare a pieno le loro doti[826].

Sono soggetti che si caratterizzanoper la loro elevata curiosità e creatività[827], ed hanno variabili livelli di competenze tecniche[828]. Possono agire da soli[829], essere collegati ad un

[824]Per vedere l'insieme dei requisiti che essi debbono soddisfare per raggiungere il summenzionato obiettivo, si veda: *Ivi,* pag. 193.
[825]Jacquet-Chiffelle,Loi, *op.cit.,* pag. 182, precisano che in realtà i cybercriminali possono anche essere i cappelli grigi perseguenti le loro ideologie, per mero divertimento ovvero i loro interessi personali. Nello stesso senso: Matulessy, Humaira,*op. cit*., pag. 142.
[826]Matulessy, Humaira, *op. cit*., pag. 142.
[827]Dai risultati riportati dagli esperimenti condotti daMatulessy, Humaira, op. cit., pag. 142,è emerso che i *black hat*(rispetto ai risultati per i *greyhat* e i *whitehat*) presentavano livelli maggiori di estroversione e di apertura alle nuove esperienze. Come però riportato daSteinmetz, *CRAFT(Y)NESS: An EthnographicStudy of Hacking*, in *The British Journal of Criminology,* 2015, vol.55, Issue 1, nelle pagg. 130-133; 138-140; http://www.jstor.org/stable/43819263/, l'hacker in generale ha una mente creativa che tende a trovare soluzioni al di fuori dei propri schemi e prova piacere quando riesce a risolvere una problematica tramite le sue abilità, completando il processo di *hacking*. I *blackhat* (ed occasionalmente anche i greyhat) però provano ulteriore piacere nell'infrangere la legge, poiché vedono come allettante l'idea di << superare quel limite che non va oltrepassato>>.
[828]Alcuni esempi sono: i *cracker*, *blackhat* o *greyhat* con elevatissime doti informatiche e/o ingegneristiche aventi l'obiettivo di accedere abusivamente nei sistemi informatici, i *phreakers*, hacker aventi l'obiettivo di accedere abusivamente nei sistemi telefonici; nonchè gli *script kiddies*, grey o black hacker aventi invece scarse doti informatiche.
[829]Un classico esempio è la figura del *cyberterrorista*(che può rientrare nella categoria degli hacker: Jacquet-Chiffelle, Loi, *op. cit.,* pag. 185) che agisce come solitario, il c.d. <<*Lone Wolf*>>, il quale <<pianifica ed

network ovvero come mercenari, vendendo strumenti o software da loro sviluppati al miglior offerente.Diversamente dai greyhat, non hanno particolare interesse nell'evitare ovvero limitare i danni conseguenti dalle loro azioni: al contrario, ritengono che l'impatto delle loro azioni nel mondo virtuale sia infinitesimale rispetto agli atti illeciti che avvengono nel mondo fisico- il che potrebbe far suggerire che <<la serietà dei loro atti non sia stata chiaramente capita, comunicata, o spiegata >>[830] a loro.

Sulla base di quanto disquisito finora, si può dunque rispondere alla prima domanda posta pocanzi: da un lato, a differenza di come frequentemente riportato dai mass media, non tutti gli hacker possono esser considerati come cybercriminali.

Dall'altro, si può affermareche i <<Black Hat>> possono esser senz'altro collocati tra i cybercriminali, poiché sempre dediti alla commissione di azioni illecite. Tuttavia, non bisogna però escludere del tutto i <<greyhat>>: piuttosto, in quel caso è preferibile eseguire una valutazione delle circostanze specifiche- senza pure escludere la possibilità che la violazione della legge sia avvenuta per errore[831].

Ulteriore aspetto da evidenziare è che le azioni degli hacker possono esser illecite, ma tuttavia accettabili secondo la morale comune (o viceversa)[832]. Ne consegue che i cittadini possono considerare che l'hacker sia un criminale quando in realtà ha sempre agito nei limiti del legale ovvero - peggio ancora– vedere le azioni dell'hacker comegiustificabili anche quando queste condotte infrangano la legge. Questo è motivo di preoccupazione e in aggiunta costituisce un forte ostacolo per la corretta individuazione dei cybercriminali.

---

esegue l'attentato in via del tutto autonoma, senza che ci siano legami con altre organizzazioni, se non di tipo ideologico>>(Lamberti, *op. cit.,* pag. 145).

[830]Silic, Lowry, *Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes*, in *Information Systems Frontiers*, 2019, Vol. 23, Is. 2, pag. 337 (DOI: https://doi.org/10.1007/s10796-019-09949-3).

[831] Contra: Steinmetz,,*op. cit*., pag.140.

[832] Basta citare sul punto: Jacquet-Chiffelle,Loi, *op.cit.,*che nelle pagg. 194-195 eseguono opportune distinzioni tra le azioni degli hacker << non rientranti nella sfera etica>>:

- L'azione <<moralmente problematica>>: viene violata con l'azione un valore morale, ma l'azione può esser giustificata <<considerando tutte le circostanze>>,
- L'azione <<debolmente immorale>>: l'azione non è la più eticamente corretta, considerate le potenziali azioni alternative rispetto alla situazione,
- L'azione <<eticamente non permessa>> (o <<fortemente immorale>>): vi è una ragione morale piuttosto solida secondo cui l'azione non andava commessa.

Oltre alla vendetta, al profitto, al divertimento ed al prestigio, tra le principali motivazioni che spingono gli hacker a compiere le loro azioni (lecite o illecite) bisogna necessariamente annoverare anche l'ideologia personale dell'individuo[833].

Utilizzando quest'ultima come criterio distintivo, si possono annoverare ulteriori tipologie di hacker[834].

In primis, bisogna trattare dei già summenzionati[835]<<hacktivisti>>[836]: si tratta spesso di <<Black hat>> di varia competenza ed abilità,caratterizzati nelle loro motivazioni da una causa che devono perseguire a tutti i costi, agendo anche contro tutti coloro che non condividono le loro metodologie ovvero la loro stessa idea. In casi più estremi, arrivano anche a pensare che solo con le loro abilità possono davvero cambiare il mondo.

Essi agiscono da soli o in gruppo e sempre in anonimato ma, diversamente da come la pensano molti altri hacker, desiderano che le loro azioni siano sempre pubblicizzate: più ampia sarà la diffusione della notizia che vi siano loro dietro gli illeciti commessi, maggiore sarà il piacere tratto dalla realizzazione della loro condotta.

Le attività illecite più comuni commesse da loro sono: gli attacchi di *Denial of Service* (di cui si parlerà in seguito[837]); i *leaks* (furto e successiva condivisione di contenuti o notizie sul web in via anticipata rispetto alla loro data di pubblicazione); le attività di *doxxing*(furto e successiva condivisione di materiale personale su pagina web); nonché il *defacing* (la modifica illecita della home page di un sito web o delle sue pagine interne).

Si deve poi proseguire trattando gli <<Internet Trolls>>[838]: si tratta di utenti dotati di grandi capacità manipolatorie ed agenti spesso in solitaria. Essi hanno l'obiettivo di provocare ovvero confondere gli altri utenti su Internet riguardo qualsiasi tematica di loro interesse (anche quella politica) tramite la diffusione di *fake news*, o pubblicando

---

[833] Uno specchio dettagliato delle motivazioni prevalenti per ogni tipologia di hacker lo si ritrova in: Seebruck, *A typology of hackers: Classifying cybermalfeasanceusing a weightedarccircumplex model*, in *Digital Investigation*, 2015, Vol.14, pag. 42. (DOI: https://doi.org/10.1016/j.diin.2015.07.002). Da queste ricerche risulta che: il gruppo Anonymous è prevalentemente motivato da vendetta, ma anche dalle ideologie; i movimenti derivanti da esso quali LulzSec e AntSec dal divertimento; mentre gli hacker mercenari sono motivati unicamente dal profitto.

[834]Pawlicka, Choraś, Pawlicki, *The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good*, in Personal and Ubiquitous Computing, 2021, Vol. 25, Is. 5, pagg. 845–850.(DOI: https://doi.org/10.1007/s00779-021-01568-7).

[835]Si dà immediato richiamo al Capitolo II, punto 1.3.2., relativo alla trattazione in generale degli autori del reato.

[836]Pawlicka, Choraś, Pawlicki*, op. cit*., pag. 845.

[837]Si rinvia direttamente al paragrafo 2.2.

[838]*Ivi,* pag. 847.

commenti d'odio ovvero di carattere controverso, nonché tramite gli *hate speech* (discorsi d'odio)[839].

Le motivazioni che inducono l'utente a perseguire tale obiettivo possono essere le più varie, ma spesso si ritrova come aspetto comune quello di attirare l'attenzione altrui o il puro divertimento- senza alcun senso di colpa per le loro azioni e con l'assoluta convinzione di esser nel giusto.

Si deve trattare infine dei <<Cyber-militanti>>[840]: utenti volontari (spesso appartenenti ai <<White Hat>>) con competenze di livello medio-basso, che agiscono sempre in gruppo organizzato volto alla commissione di attacchi cibernetici a livello propagandistico ovvero per la promozione di un ideale politico. Possono anche essere assoldati direttamente dagli Stati [841], ma – a differenza dei c.d. <<State - Sponsored hackers>> [842] - agiscono gratuitamente e i loro attacchi non sono necessariamente rivolti contro altri Stati.

In conclusione, da quest'ulteriore classificazione si comprende sia come l'hacker sia una figura camaleontica, per la quale è necessaria una opportuna valutazione caso per caso sulla sua figura e sulla condotta posta in essere in concreto, sia che - rispondendo alla seconda domanda posta lungo il corso di questa discussione – è ben possibile che egli diventi partecipante di un'organizzazione, sia di tipo lecito che illecito.

---

[839]Seppur ancora gli studi sul campo siano piuttosto recenti, è ben certo che l'espressione dell'odio non è rilevante ai fini giuridici *tout court*:questo sia perché sia entrano in gioco valori etici, sociali e politici in costante evoluzione, ma anche perché disporre una normativa volta alla censura di qualsiasi manifestazione d'odio andrebbe sicuramente contro la libertà di manifestazione del pensiero. Seppur entrambi i casi rientrano nelle manifestazioni d'odio, è sufficiente indicare in questa sede che risultano essere due elementi aventi un peso diverso da un punto di vista giuridico, utili a distinguere tra "commenti" e "discorsi"d'odio: se gli *hate speeches* sono un genere di discorsi che esprimono odio ed intolleranza verso una persona o un gruppo tali da comportare reazioni violente, contro i quali esiste un'apposita disciplina penale - nazionale e sovranazionale-, i commenti d'odio non risulterebbero essere punibili penalmente, sia perché la linea tra il singolo commento esprimente il mero dissenso e quello eseguente la denigrazione è piuttosto labile, ma anche perché (a differenza degli *hate speech*) i commenti d'odio online non si mantengono a lungo nel tempo e non si ripresentano in diversi formati, poiché il <<tono>> dei commenti è strettamente dipendente dall'interesse della community- si parla infatti in quel caso di <<odio esposto>>. (Ziccardi, *L' odio online : violenza verbale e ossessioni in rete*. R. Cortina, 2016, pag. 16). Per maggiori approfondimenti, si veda: Di Tano, *L'odio in rete,* in Casadei,Pietropaoli, *Diritto e Tecnologie informatiche* CEDAM, 2021, pag.168-178; Pezzella, *La diffamazione*, UTET Giuridica, pagg. 1046 ess.; Lugato, *Il <<discorso d'odio>>. Le coordinate giuridiche del ragionamento internazionalistico,* in *Riv. Dir. Int.*, fasc.4, 2022, pag. 959 e ss. .

[840]Traduzione di <<Cyber-militants>>, ripresa in: Pawlicka, Choraś, Pawlicki*, op. cit*., pag. 848 e ss.

[841] Pawlicka, Choraś, Pawlicki*, op. cit*., pagg. 848- 849, quali riportano che i cyber militanti sono frequentemente assoldati da Stati come la Russia, l'Estonia, gli Stati Uniti, la Cina.

[842]Gli <<State-Sponsoerd Hackers>> sono hacker di gran competenza che vengono assunti dal governo dello Stato per destabilizzare o distruggere i sistemi di un governo o di uno Stato diverso. Per ulteriori approfondimenti, si cita: Ahmad, Webb, Desouza, Boorman, *Strategically motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack*, n *Computer Security,* 2019, Vol. 86, pagg.402- 418; Broadhurst, Grabosky, Alazab, Chon, *op. cit*., pagg. 15-16.

2. *Il profilo organizzativo: le comunità virtuali.*

Così come è dimostrato che l'ambiente sociale può rivelarsi determinante per la formazione dei potenziali criminali, il territorio del ciberspazio è luogo fertile per l'espansione del raggio d'azione delle organizzazioni fisiche, ma soprattuttodi nascita e di sviluppo anche di quelle esclusivamente virtuali- specie se i membri appartengono a Stati distanti tra loro[843]. È dunque fondamentale disquisire sulle comunità virtuali, dalle cui modalità di interazione può dipendere quale sarà la tipologia d'elemento organizzativo che si porrà in essere[844].

Il realtà, la vera difficoltà nel disquisire questo argomento consiste nel comprendere la linea di confine tra le mere conversazioni online e la creazione e sviluppo di un'organizzazione, sia per l'obiettiva difficoltà di individuare l'esatto momento del passaggio dal mero messaggio all'accordo, sia perché si può avere come esito un accordo a dar vita ovvero ad aderire organizzazioni ben strutturate e di carattere permanente (anche di carattere mafioso), ma anche un accordo temporaneo e specificamente rivolto alla commissione sulla rete cibernetica di uno o più delitti[845]. Ma bisogna fare un passo indietro.

L'uomo è un animale sociale, sempre alla ricerca di nuove interazioni sia nella realtà fisica che in quella virtuale[846], in costante movimento e con un incessante mutamento degli argomenti di conversazione e degli utenti - a maggior ragione se avviene online, che si connota per la rapidità nello scrivere e l'arrivo del messaggio ai destinatari in tempi simultanei.

Quest'aspetto ha determinato la caratteristica della flessibilità degli eventuali gruppi organizzati, ossia la non indispensabilitàd'una struttura gerarchica prestabilita per il suo

---

[843]Leukfeldt,Kleemans, Stol, *Cybercriminal networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks*, in *British Journal of Criminology*, Vol. 57,Is.3, (DOI:.https://doi.org/10.1093/bjc/azw009)a pagg.719-720, hanno rilevato che, con riferimento alle organizzazioni a delinquere olandesi specializzate nel *phishing*, i network hanno avuto un ruolo fondamentale per abilitare nuovi co-offensori residenti in altri Stati, per aumentare le loro tecniche criminali ovvero implementare gli strumenti utilizzati, nonché anche la possibilità di mettersi in contatto con dei nuovi potenziali membri.

[844]Lo sostiene Bussolati, *op. cit.*, pag. 257, portando, come es.: *i forum*, dove i messaggi si strutturano su una tematica di discussione; le *newsletter*, un insieme di e-mail che arrivano periodicamente; le *chat*, che <<ammettono la creazione di varie "stanze" (o "canali") per la comunicazione […]>>, consentendo dunque agli utenti una maggiore libertà nella scelta delle tematiche di cui conversare.

[845]Si richiama il punto 2.1. del Capitolo I, dove - come si è già visto – trattandosi di un accordo ex art. 115 c.p., si esclude in quel caso la presenza di un'associazione a delinquere, poiché manca la <<capacità a perdurare>> caratterizzante il vincolo associativo.

[846] McAlaney, *Are you anonymous? Social-psychological processes of hacking groups*, in AA.VV., *Cybersecurity and Cognitive Science*, (a cura di) Moustafa, 2022, Academic Press, pag.152 (DOI: https://doi.org/10.1016/B978-0-323-90570-1.00003-6).

funzionamento (salvo casi particolari[847]), realizzando dunque <<un taglio netto rispetto alla composizione gerarchica tipica del crimine organizzato tradizionale>>[848].

Questa flessibilità però non deve essere intesa in senso estremo: è emersa la presenza di un esiguo nucleo di cybercriminali online gestenti le piattaforme in cui avvengono queste comunicazioni. La loro posizione non è per nulla da sottovalutare: essi sono non solo in grado di divenire un punto di riferimentoper i diversi utenti visitanti le piattaforme, ma sono anche spesso dotati di poteri decisionali sull'eventuale esclusione degli utenti e sulle tematiche di discussione, potendo far dirigere facilmente l'attenzione di massa dei partecipanti sulle operazioni illecite che intendono compiere.

Tuttavia, altri elementi chiave di questi fenomeni quali: la grande difficoltà d'identificare tra essi il capo, la capacità di ogni singolo membro di assumere diversi ruoli e funzioni a seconda delle necessità e delle azioni da compiere anche contemporaneamente e le costanti interazioni tra membri di gruppi diversi tra loro (anche per una potenziale collaborazione per la commissione di specifici reati) rende quasi impossibile definire compiutamente il modello organizzativo come flessibile ovvero rigidamente gerarchico.

In definitiva, si potrebbe definire l'elemento organizzativo delle associazioni a delinquere esclusivamente online come una <<rigidità flessibile>>[849]: una costante mutevolezza e notevole capacità di ramificazione, ma con la compresenzad'un nucleo centrale fisso e solido.

Quanto detto sopra è confermato dalle due tipologie di modalità d'organizzazione di associazioni a delinquere esclusivamente cibernetiche più comuni[850]:

1. Lo <<sciame>>[851]: corrisponde ad un gruppo disorganizzato senza alcuna figura di capo, i cui membri sono uniti solo da un'ideologia o obiettivo comune il cui numero è elevato ma

---

[847] Tropina, *op. cit.*, pag. 53, fa riferimento all'ipotesi di criminalità organizzate gestenti un mercato illecito:considerato che solo persone meritevoli di fiducia possano effettivamente accedere alla piattaforma online in cui poter acquistare i proventi di carattere illeciti, è necessario per esse una struttura organizzativa sofisticata in grado di poter disporre sia dei meccanismi di selezione ai potenziali membri, sia di controllo delle loro attività.

[848]Tropina, in *Organized Crime in Cyberspace*, in: Stiftung, Schönenberg, *Transnational Organized Crime. Analyses of a Global Challenge to Democracy*, 2013, Transcript Verlag (https://www.jstor.org/stable/j.ctv1fxh0d.8), a pag.53 fa un esplicitoriferimento a: AA.VV., *Threat assessment (abridged). Internet facilitated organised crime*, document dell'Europol - iOCTA. The Hague, 07/01/2011. (https://www. europol.europa.eu/sites/default/files/publications/iocta.pdf).

[849]Per questa definizione,si è preso spunto da:Dore, *Flexible Rigidities. Industrial Policy and Structural Adjustment in the Japanese Economy, 1970-1980,* 1986, Bloomsbury.

[850]Broadhurst, Grabosky, Alazab, Chon, *op. cit*., nellepagg. 5-6 citano: McGuire, *Organised crime in the digital age*, John Grieve Centre for Policing and Security and BAE Systems Detica,2012,http://www.baesystemsdetica.com/uploads/resources/ORGANISED_CRIME_IN_THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf).

sempre sfuggente, considerando che non sono previsti particolari controlli eseguiti su chi entra o esce. Questa è la classica tipologia di organizzazione dei gruppi degli hacktivisti - organizzazione Anonymous *in primis.*

2. Gli <<hubs>>: sono caratterizzati da un <<nucleo>> fisso di cybercriminali e da collegamenti periferici, consistenti nel legame con altri cybercriminali - aventi a loro volta ulteriori collegamenti con altri utenti ovvero facenti parte di ulteriore organizzazione[852], e così via. A differenza del precedente gruppo, il legame tra i membri è molto più forte e frequente.
   Questa conformazione si ritrova spesso nelle organizzazioni criminali dedite al furto, alla clonazione ed al traffico di carte di credito online[853].

Comparando queste tipologie di organizzazione di associazioni a delinquere con quelle <<ibride>>, si deve accennare al fatto che in quest'ultime, diversamente da quanto visto sopra, è sempre presente una gerarchia (anche di livello minimo). Conseguentemente, relativamente alle associazioni a delinquere esclusivamente cibernetiche, se si riprendessero in considerazione gli elementi del fatto tipico così come indicati nell'art. 416 c.p.[854], si dedurrebbe che l'elemento organizzativo verrebbe quasi messo in secondo piano dal vincolo associativo (l'entrata nelle comunità online, la partecipazione alle conversazioni, la comprensione della natura illecita delle conversazioni stesse e la scelta di aderire a proposte di carattere illecito ovvero a proporle direttamente) e dal programma (gli obiettivi comuni ovvero l'ideologiadella comunità onlineda perseguirsi attraverso la commissione di illeciti penali).

Questa ridimensionata importanza dell'elemento organizzativo emergerebbe anche da altri due elementi.

---

[851]Diretta traduzione di <<Swarms >> eseguita da: Broadhurst, Grabosky, Alazab, Chon, *op. cit*., pag.5.
[852]Tropina, *op. cit.*, pag. 54, fa appunto riferimento a come i forum online (ad esempio, il Dark Market) possano divenire un mezzo di mediazione fondamentale tra le organizzazioni e/o i singoli cybercriminali ma anche siano un ottimo strumento per esibire le loro doti informatiche, in modo da attrarre potenziali criminali per la commissione di nuovi reati ovvero per poter scambiare informazioni.
[853]Broadhurst, Grabosky, Alazab, Chon, *op. cit*., pag.5.
[854]Si richiama al paragrafo 2 del Capitolo I.

Il primo consiste nell'elenco dei <<ruoli >> più abitualmente presenti[855] (che, come ricordato sopra, possono esser ricoperti contemporaneamente dalla stessa persona ovvero da più persone all'interno del gruppo). Elencando alcuni esempi:

- I programmatori, che eseguono la creazione e la preparazione dei software, malware e degli altri strumenti necessari per la commissione del delitto,
- I distributori: si occupano dello scambio e della vendita dei dati e del contenuto rubato, e garantiscono agli ingenui destinatari che il materiale non abbia alcuna provenienza illegale,
- I tecnici, che hanno il compito di sistemare e costantemente aggiornare la struttura informatica e tutti i sistemi di supporto,
- Gli esperti in frode informatica, tenuti a sviluppare nuovi schemi ingegneristici di carattere fraudolento (se si ha a che fare con associazioni a delinquere cibernetiche specializzate nel phishing o nell'estorsione);
- Coloro che interagiscono col pubblico esterno, sia per il reclutamento di nuovi utenti, sia direttamente con le vittime: nonostante sia un'attività eseguita da quasi tutti i membri, nelle organizzazioni più specializzate il compito è affidato a chi dimostra di avere buone capacità persuasive ed abilità manipolatorie. Si potrebbe dunque avvicinare alla figura del promotore ex art. 416 c.p.;
- Gli <<esecutivi>>: coordinano il flusso delle attività criminali e possono sollecitare il gruppo ad orientarsi su determinate tematiche piuttosto che altre, in modo da decidere insieme quali possono esser gli obiettivi da perseguire.

È interessante notare che questo stesso elenco ha subito delle critiche, perché eccessivamente rivolto a descrivere le organizzazioni criminali operanti online <<come se fossero delle aziende>>[856] ben strutturate e rivolte alla sola commissione di frodi informatiche: oltre al vasto numero di tipologie di reati non tenuti in considerazione, questa specializzazione è particolarmente raranelle associazioni a delinquere operanti esclusivamente online.

Si aggiunge anche che dallo stesso elencoemerge l'impossibilità di riconducibilità dei ruoli dei singoli utenti ad una struttura ben chiara e definita (anche di livello minimo). Questa lacuna è probabilmente dovuta all'interscambiabilità dei ruoli stessi.

---

[855] *Ivi,* pagg. 7-8, nello studio in particolare delle associazioni a delinquere finalizzate alla truffa online, fanno diretto riferimento alle ricerche di: Chabinsky, *The Cyber Threat: Who'sDoingWhat to Whom*?, cit., pubblicato il 25/03/2010 sul sito ufficiale dell'FBI. http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom .

[856] *Ivi.*, pag. 16.

Il secondo aspetto da tenere in considerazione è relativo alle possibili misure da prendere contro queste forme di criminalità sul piano cibernetico: viene particolarmente evidenziato il fatto che non si dia abbastanza importanza a<<chi ci sia dietro il gruppo>>[857], dedicando poca attenzione al gruppo come entità unitaria.

Non che l'individuazione dell'utente nella vita reale sia un dato da trascurare, ma si deve far notare come,dagli studi trattati finora,vi sia una focalizzazione solo sulla figura del membro delle organizzazioni criminose online, lasciando sullo sfondo l'elemento organizzativo stesso: questo è un dato che non fa altro se non dimostrare ulteriormente la subordinazione dell'elemento organizzativo delle associazioni a delinquere esclusivamente online rispetto agli altri due elementi del fatto tipico- come visto nelle pagine precedenti.

Riprendendo l'analisi delle diverse problematiche della fattispecie dell'associazione a delinquere ex art. 416 c.p., è curioso notare, invece, come emerga il caso opposto: l'eccessivo riferimento all'elemento organizzativo da parte della dottrina e della giurisprudenza italiana, in grado d'oscurare gli altri due elementi costituenti il fatto tipico dell'associazione a delinquere semplice.

3. Brevi cenni alle associazioni a delinquere finalizzate allo scambio di materiale pedopornografico da un punto di vista criminologico e penale.

Le associazioni a delinquere rivolte alla pedopornografia online (più specificamente,alla <<produzione, diffusione e commercio in Internet di materiale pedopornografico>>[858]), parrebbero essere una delle forme di associazioni a delinquere online oggettodi più grande discussione nel panorama internazionale[859] e su cui si è più frequentemente pronunciata la giurisprudenza italiana[860].

Considerando sia la possibilità di operare in anonimato che l'istantaneità delle comunicazioni nel mondo cibernetico, è avvenuto un vero e proprio passaggio della

[857]Tropina, *op. cit.*, pag. 54.
[858] De Vivo, Ricci, *op. cit.,*pagg. 36-37. Nello stesso senso: Bussolati, *op.cit.*, pag. 257-8
[859]Bussolati, *op.cit*, pag. 258, fa riferimento a : AA.VV.,*The State of the World's Children in a digital world,,* Report dell' UNICEF 2017, pagg.76-90 (https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf).
[860]Picarella, *op. cit.,* pag. 314, ma della giurisprudenza e legislazione italiana se ne tratterà ampiamente in seguito nel testo.

pedofilia da fenomeno isolato a ~~v~~ero e proprio mercato criminale, dove i consumatori dei contenuti possono anche assumere loro stessi le vesti di produttori, potendo caricare loro stessi materiale in siti, in modo da poter soddisfare tutte le fantasie più sfrenate[861].

Facendo un breve criminalprofiling dei partecipanti a queste associazioni a delinquere, si tratta quasi sempre di maschi adulti (di età media di 35 anni)[862] partecipanti in anonimato e che non si incontrano mai di persona[863]. Inoltre, ulteriori tratti comuni sono la forte presenza di disturbi psicologici coniugati alla consapevolezza dell'illiceità delle loro condotte: non a caso si è riscontrato che, in base alle ricerche condotte, molti tra loro hanno ammesso di soffrire di depressione quando eseguivano le loro attività illecite[864]. Si riscontra anche che questi soggetti usualmente tendono a far parte delle minoranze sessuali o a non avere dei rispettivi partner nella loro vita amorosa.[865]

Sulla base delle recenti ricerche criminologiche, si possono ritrovare in queste associazioni a delinquere tre diverse tipologie di pedofili[866]:

1. Il << pedofilo voyeuristico>>[867]: corrispondente alla maggioranza dei soggetti esaminati (circa l'89% del campione), si tratta dell'utente interessato al solo consumo di materiale pedopornografico, senza mai un contatto fisico con i minori;
2. Il <<pedofilo misto>>,il quale utilizza abitualmente materiale pedopornografico, ma ha anche contatti fisici con minori (sia in via occasionale che frequente), posti in essere o all'interno della famiglia o in seguito ad avvicinamento causale;

---

[861]Niveau, *op.cit.,* pag. 573. Nello stesso senso: De Vivo, Ricci, *op. cit*., pagg. 37.

[862] *Ivi,* pag.571. Nello stesso senso, riguardo la figura del pedofilo italiano online, si veda:Telefono Arcobaleno ONLUS - Centro studi e ricerche sull'abuso d'infanzia, *International Observatory Against Child Abuse and Sexual Exploitation,Short Report*- April 2011; pag.4. (https://www.dmi.unict.it/~battiato/CF1011/ShortReport-aprile2011.pdf)

[863]Picarella, *op. cit.* ,pag. 314. Nello stesso senso: De Vivo, Ricci, *op. cit*, che aggiungono come infatti il computer diventi <<la carta di identità del pedofilo>>: da esso si può risalire facilmente al materiale di scambio dell'utente, alle sue preferenze sessuali, ai contatti che effettua, alle ore del giorno che trascorre on-line.

[864]Niveau, *op.cit.,* pag. 572, ha identificato infatti, che dei 36 partecipanti ai suoi studi, ben 30 avevano ammesso di esser consapevoli dell'illiceità delle loro azioni, e più del 70% dei partecipanti avevano manifestato disordini della personalità. Di questi ultimi, 7 avevano ammesso di aver sofferto (o di soffrire) di depressione quanto tenevano i loro comportamenti, ma di non essersi rivolti ad alcuno psichiatra per i loro disturbi.

[865]*Ivi,* pag.573, fa riferimento a: Hall, Hall, *A profile of pedophilia: definition, characteristics of offenders, recidivism, treatment outcomes, and forensic issues*, cit., in *Mayo Clinic proceedings, 2007,* Vol. 82,Is.4, pagg. 457-471. (DOI:https://doi.org/10.4065/82.4.457).

[866]De Vivo, Ricci, *op. cit*., pag41, fanno riferimento agli studi condotti sulla pedofilia in Italia da Strano, *Manuale di criminologia clinica*, 2003, SEE Ed., pagg. 375 e ss. Sulla base del Report eseguito dal Centro Studi Telefono Arcobaleno nel 2011 (Telefono Arcobaleno ONLUS- Centro studi e ricerche sull' abuso sull'infanzia, *International Observatory Against Child Abuse and Sexual Exploitation,* Short Report- April 2011), emerge che l'Italia non è un Paese produttore di materiale pedopornografico, ma risulta essere in Europa al quarto posto tra gli Stati facenti domanda di esso: sul punto v.De Vivo, Ricci, *op. cit*.,pag.39.

[867]De Vivo, Ricci, *op. cit*.,pag.39.

3. Infine, vi è il <<pedofilo abusante>>: di carattere estremamente raro, corrisponde al pedofilo che esegue come attività predominante l'abuso fisico sui minori. Inoltre, è di solito anche <<ricercato attraverso la prostituzione minorile e il "turismo sessuale">>[868].

Trattando poi quelli che sono gli strumenti informatici e cibernetici maggiormente utilizzati, l'accesso al materiale pedopornografico può avvenire tramite siti web (previa iscrizione e/o pagamento) ovvero in apposite chat o forum di discussione, dove gli utenti si scambiano gli appositi link ed i codici d'accesso. I mezzi però più frequentemente utilizzati dalle comunità online pedopornografiche sono: le attività di archiviazione dei dati via Rete (il c.d<<*online storage*>>[869]) o tramite hard disk virtuali-in entrambi i casi, sempre protetti da password- nonché i servizi *peer to peer* (P2P), in grado di consentire ai soggetti la condivisione e lo scambio di materiale senza attività d'intermediazione o la connessione ad un apposito sito web[870]. Infine, i pagamenti avvengono attraverso transazioni on-line gestite da siti di diversi paesi[871]ovvero si utilizzano degli abbonamenti attraverso i quali l'utente ottiene una password con la quale può accedere ai siti pedopornografici per un lasso di tempo.

Prima di chiudere in via definitiva la parte criminologica, è importante precisare che tutti questi strumenti e mezzi citati finora sono presenti sia nel Clear Web che nel Dark Web[872].

Passando adesso alla trattazione dell'argomento da una prospettiva giuridica, le disposizioni normative italiane contro la produzione e diffusione di materiale pedopornografico tramite i siti informatici e cibernetici sono state frutto d'un lungo *excursus*[873]legislativo ma, al fine di comprendere meglio quali elementi sono stati presi in

---

[868]*Ivi*, pag. 41.

[869]*Ivi,* pag. 37.

[870]Bussolati, *op. cit*., pag. 259. V. pure De Vivo, Ricci, *op. cit*., pag. 38.

[871]De Vivo, Ricci, *op. cit*., pag. 38, fanno riferimento appunto a server americani, olandesi, russi, ucraini e tedeschi, nel quale si fa utilizzo della carta di credito per le transazioni.

[872]Bussolati, *op.cit*., pag. 259.

[873]Si elencheranno di essa i punti più salienti:

- La legge n. 269/1998 (<<Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù>>, ha introdotto nel Codice Penale gli artt. da 600-*bis* a 600-*septies,* imponendo misure di contrasto importanti alla pedopornografia online, dando un quadro di completezza alla Legge n. 66/1996 (<<Norme sulla violenza sessuale>>). Tuttavia, la nozione di pornografia ricavata dall'art. 600-*ter* (relativa solo a <<veri e propri atti sessuali del minore>>: v. De Vivo, Ricci, *op. cit*., pag. 33) e l'orientamento principale della giurisprudenza sull'articolo in questione eccessivamente restrittivo rendevano necessari nuovi interventi legislativi.
- Il legislatore ha perciò emanato la legge n. 38/2006 (<<Disposizioni In materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet>>,Gazzetta Ufficiale n. 38 del 15/02/2006,https://www.gazzettaufficiale.it/eli/gu/2006/02/15/38/sg/pdf) allo scopo di colmare le lacune

considerazione per la riconducibilità di questa forma di associazione a delinquere all'ambito di applicabilità dell'art. 416 c.p., bisogna necessariamente volgere lo sguardo ad alcune pronunce della giurisprudenza italiana[874].

La prima pronuncia che ha tentato l'applicazione di questa fattispecie a queste comunità online è quella della Terza Sezione della Cassazione Penale nel 2004[875], <<relativa alla distribuzione e divulgazione per via telematica di foto pedopornografiche>>[876].

La Corte, dopo uno sforzo non indifferente, alla fine rispose in via affermativa nell'applicazione dell'articolo 416 c.p. rispetto alla fattispecie concrete, poiché ritenne che sussistessero, nell'ordine:

- L'elemento oggettivo: la comunità virtuale è << stabile ed organizzata>>, nonché <<regolata dalle disposizioni dettate dal promotore e gestore, volta allo scambio ed alla divulgazione […] di foto pedopornografiche>>[877];
- L'elemento soggettivo, consistente nel fatto che i membri erano consapevoli <<dello scopo e delle finalità del gruppo>>, assieme <<all'impegno di inviare periodicamente altre foto pedopornografiche.>>[878].

---

preesistenti ma anche per conformarsi alla disciplina penale posta a livello europeo per la tutela dei minori contro la pedopornografia (compreso anche l'utilizzo del mezzo informatico).Dietro la legge vi era l'obiettivo di <<frenare la circolazione di materiale pornografico con le reti informatiche ed evitare l'estensione della violenza sessuale nei confronti dei minori>>, sulla base del presupposto che le immagini virtuali potessero incentivare la pedopornografia e la pedofilia. Anche questa normativa è stata però ampiamente criticata, specie sull'aspetto eccessivamente severo da un punto di vista sanzionatorio, sia per la difficoltà effettiva dell'individuazione del bene giuridico.

- Infine, si menziona la legge n. 172/2012 (<<Ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007, nonché norme di adeguamento dell'ordinamento interno>>), con la quale si è ratificata la Convenzione di Lanzarote, e che ha predisposto numerose modifiche al codice penale e processuale penale italiano: fra tutte, si segnala l'introduzione nell'art. 416 c.p. del settimo comma, volto all'aggravamento della pena per l'associazione a delinquere semplice se essa è rivolta alla commissione dei reati compresi tra il 600-*bis* ed il 600-*undecies* c.p.

[874] Nonostante ancora la tematica sia piuttosto recente, si segnala la presenza di sentenze più recenti rispetto a quelle oggetto di trattazione. Si cita, ad es.: Cass. pen. sez. IV n.593/2022; Cass. pen. sez. III, n.12525/2022,Cassazione penale sez. III, n.37541/2019.

[875]Cass. pen.,Sez. III, n. 8296/2004, in *Cass. pen*., 2006,Vol. 5, pag.1819.

[876]Bussolati, *op. cit.,* pag. 259.

[877]Cass. pen.,Sez. III, n. 8296/2004, in *Cass. pen*., 2006,Vol. 5, pag.1819.

[878]Cass. pen.,Sez. III, n. 8296/2004, in *Cass. pen*., 2006,Vol. 5, pag.1819.Si aggiunge che(cfr. anche: Cassazione penale Sez. V, n.10076/1998, Rv. 213979), poiché l'art. 600-ter c.p.(che punisce la pornografia minorile) è un reato di pericolo concreto, in questa sentenza si affida alla discrezionalità del giudice l'accertamento della sussistenza del pericolo nel caso specifico, facendo riferimento ad elementi della condotta come: l'esistenza di una struttura organizzativa anche rudimentale atta a corrispondere alle esigenze di mercato dei pedofili, il collegamento dell'agente con soggetti pedofili (potenziali destinatari del materiale pornografico), la disponibilità materiale di strumenti tecnici di riproduzione e/o trasmissione, anche telematica, idonei a diffondere il materiale pornografico in cerchi più o meno vasti di destinatari, l'utilizzo contemporaneo o differito nel tempo di più minori per la produzione del materiale pornografico, i precedenti penali, la condotta antecedente e le qualità soggettive del reo.

Segue poi una sentenza del Tribunale di Siracusa nel 2012[879] relativa ad un sito web di pedopornografia,con l'ulteriore utilizzo da parte dei membri della piattaforma MSN per lo scambio e condivisione di materiale pedopornografico. Gli aspetti interessanti in questo caso sono: la presenza di un regolamento a cui ogni membro doveva attenersi, nonché la presenza di una minima struttura gerarchica (vi era il creatore ed il gestore del sito, che aveva il potere di prendere le decisioni relative all'accesso ed espulsione dei membri, mentre tutti gli altri erano solo meri iscritti, tenuti alla condivisione del materiale pedopornografico)[880].
Sulla base di questi elementi a disposizione e sulla pronuncia precedente, il Tribunale di Siracusa ha ritenuto che la comunità virtuale in questione avesse gli elementi sufficienti per esser ricondotta all'associazione per delinquere semplice.

Bisogna infine citare la sentenza della Terza Sezione della Cassazione del 2013[881] relativa ad una comunità online dedita allo scambio di materiale pedopornografico, nonché alla gestione di un enorme archivio virtuale composto da un numero elevato di file.
Secondo il dispositivo, anche questa comunità agiva in anonimato ed era dotata di una solida gerarchia, di regole ferree relative allo status di membro, ed in aggiunta anche <<di […] specifici sottogruppi>>[882]: da tutti questi elementi non era difficile ritenere sussistente sia l'elemento del vincolo associativo che quello organizzativo del fatto tipico ex art. 416 c.p.
Inoltre, per l'aspetto soggettivo, si afferma in sentenza che la volontà consapevole di partecipazione era facilmente ricavabile dal fatto che <<la partecipazione al gruppo era ammessa solo dopo l'esplicita accettazione del gruppo>>[883] e dall'impegno costante di condivisione di materiale pornografico da parte dei membri.
Inutile dire che, a distanza di quasi dieci anni, questa sentenza si pronuncia <<sul solco di quanto delineato nella Sentenza del 2004>>[884].

Sulla base di quanto emerso finora, si possono eseguire diversi ragionamenti relativi sia sull'elemento oggettivo che soggettivo della fattispecie. Partendo dal fatto tipico, emerge

[879]Tribunale di Siracusa, n. 229/2012, in *Giur. di Merito* 2013, fasc.11, pag.2428.
[880] Questa figura di vertice si faceva chiamare "il padrone". Quest'ultimo accentrava a sé ogni potere decisionale, mentre i semplici iscritti erano tenuti a caricare materiale pedopornografico per mantenere il loro status di membro.
[881]Cassazione penale sez. III,n. 20921/2013, in CED Cassazione penale 2013. In senso conforme: Cass. pen., sez. V, n. 10076/1998 ,Rv. 213979.
[882]Bussolati, *op. cit.,* pag. 261;
[883]*Ibidem.*
[884]*Ivi,* pag. 260.

immediatamente come la conoscenza del previo programma, la formale adesione ad esso ed il continuo contributo fornito dal membro permette la rilevazione del vincolo associativo (nonché la presenza dell'elemento doloso della condotta).
Riguardo poi l'elemento del programma, a differenza delle altre ipotesi <<tradizionali>> dell'associazione a delinquere, dove il programma non sempre si trova in un apposito documento dettagliato[885]; qui, al contrario, il programma dell'associazione ed il suo statuto sono sempre dettagliatamente specificati in appositi documenti: essi diventano quasi una sorta di <<«manifesto» associativo>> [886] , in grado di far segnalare la presenza dell'associazione in Rete, attraendo gli utenti che condividano gli obiettivi ed i metodi utilizzati dall'organizzazione stessa.
Da ultimo, c'è una struttura organizzativa molto solida, basata su <<un rigido sistema normativo>>[887], regolante l'accesso, lo status e l'espulsione dei membri. Inoltre, in certi casi, si riesce pure ad individuare facilmente le figure apicali e/o i gestori di queste comunità virtuali;

Passando poi alla configurazione della condotta di partecipazione di questi membri, sono sorti dubbi da parte della dottrina sul propendere, in queste fattispecie concrete, per il modello organizzativo (il soggetto diventa partecipante con la mera adesione) ovvero prediligere il criterio causale (il soggetto diventa partecipante non solo con l'adesione, ma anche conil contributo causale che arreca all'associazione - nel caso specifico, con la produzione e condivisione del materiale pedopornografico).
Tendenzialmente si dovrebbe propendere più per il modello causale, considerato che può accadere che il soggetto abbia un intento diverso dalla pura e semplice adesione, comead es. << […] procurarsi il materiale pedopornografico custodito nello spazio […]virtuale, senza voler realmente aderire agli scopi criminosi dell'associazione, né tantomeno voler contribuire al suo consolidamento o alla sua espansione >>[888].

Visto che la scelta del modello causale può tuttavia facilmente portare a desumere la corrispondenza tra fattispecie astratta e concreta avendo come riferimento pochi elementi concreti (dando a non pochi problemi applicativi - come si è avuto modo di osservare precedentemente[889]), bisogna segnalare un'interessante posizione al riguardo, incentrata

[885]Si richiama, a tal proposito, il Capitolo I, paragrafo 2.2.
[886]Stramaglia, *L'associazione per delinquere nell'era della realtà virtuale*, (nota alla sentenza Trib. Siracusa, n. 229/2012), in *Giur. di Merito*, 2013, fasc.11, pagg. 2436-2437.
[887]Bussolati, *op. cit.,* pag. 261.
[888]Stramaglia*, op. cit*., pagg. 2438-2439.
[889]Si richiama, a tal proposito, il Capitolo I, punto 3.1.

sull'utilizzo di entrambi i modelli: la partecipazione dovrebbe infatti esser vista come <<una condotta oggettivamente e soggettivamente complessa>>, caratterizzata da una <<unione di forze per imprese precluse agli sforzi individuali>>[890]: perciò, l'impegno di partecipazione deve – letteralmente- esser espresso sia a paroleche con i fatti.

Le difficoltà e le contraddizioni emerse nel tentare di inquadrare i caratteri delle associazioni per delinquere operanti onlineben si comprendono se si riporta alla mente quanto detto sulla fatica degli studiosi (giuristi, criminologi, psicologici e sociologi) nell'arrivare a comporre un quadro generale ed unitario relativo alle diverse forme di delinquenza presenti nel sistema cibernetico ed informatico.
Perciò, si ritorna sempre al punto di partenza visto nel capitolo dedicato al cybercrime in generale: il costante mutamento del mondo cibernetico dove si colloca la criminalità, porterà ad infinite variazioni nei aspetti essenziali delle fattispecie di reato– associazione a delinquere compresa.

Questo emergerà palesemente nella trattazione nel prossimo paragrafo riguardante l'associazione a delinquere Anonymous, dove – a differenza delle associazioni a delinquere online finalizzate allo scambio e distribuzione di materiale pedopornografico - la difficoltà d'individuazione degli elementi del fatto tipico ex art. 416 c.p. sarà evidente.

4. L'associazione a delinquere online finalizzata all'attacco informatico. Il caso Anonymous.

«Chiunque voglia può essere Anonymous e lavorare per una serie di obiettivi... Abbiamo un programma su cui tutti concordiamo, ci coordiniamo e agiamo, ma per la sua realizzazione tutti agiscono indipendentemente, senza volere alcun riconoscimento. Vogliamo solo raggiungere qualcosa che crediamo sia importante...»[891]

In questo paragrafo finale si cercherà di analizzare una delle associazioni a delinquere esclusivamente cibernetica,<<hacktivista>>, e tra le più note e diffusa al mondo: l'Associazione Anonymous. Ma, prima di procedere con la trattazione, bisogna fare una piccola ricostruzione storica, dando uno sguardo anche a quelle che sono state le loro

[890]*Ivi,* pag 2440, fa riferimento a: Lattanzi,Lupo,*Codice penale. Rassegna di giurisprudenza e di dottrina*, cit., 2010, vol. IX, Giuffrè, pag. 82.
[891]Dichiarazione di un membro di Anonymous citata nell'articolodi Landers, *Serious business: Anonymous takes on Scientology (and doesn't afraid of anything)*, *in Baltimore City Paper* n.4,pubblicato il 2/04/2008.

principali azioni compiutefino ad oggi- comprese quelle eseguite dal gruppo Anonymous italiano.

Bisogna tornare indietro nel 2003, quando venne creato dall'allora quattordicenne inglese Poole il sito 4chan.org[892], al fine di avere un sito dove poter parlare liberamente degli argomenti più disparati. Caratteristica basilare del sito era che i contenuti pubblicati erano sempre caricati in via anonima(la c.d. <<*Anon mode* >>, dalla quale deriva lo stesso nome dell'organizzazione). All'interno del sito vi erano diversi forum di discussione in ordine alfabetico in base alle diverse tematiche di discussione, ma quello che sarebbe più diventato più popolare è /b/, <<il forum "random">>[893].

In esso sarebbe stato possibile non solo spaziare su tematiche non propriamente lecite e di carattere moralmente discutibile[894](es. violenza, bullismo, pornografia) ed utilizzare un linguaggio comprensibile solo ai partecipanti, ma anche far in modo che – nonostante la velocità delle conversazioni - un intervento fosse in grado di <<spingere altri [partecipanti del forum, n.d.a.] a mettersi insieme per uno scherzo di massa o "raid">>[895] . Sarà proprio questo forum a diventare la culla della futura organizzazione Anonymous.

Inizialmente il gruppo eseguiva qualche scherzo sulweb[896] al mero scopo di <<lulz>>[897], ma la prima vera e propria operazione complessa e particolarmente organizzata furono i diversi attacchi di Denial of Service - in abbreviazione, <<DoS>>-contro il sito web

[892] Il sito è tutt'oggi esistente: https://4chan.org/. In base a quanto ricercato, risulterebbe essere incentrato più che altro su discussione di anime e manga giapponesi (in base quindi all'originario <<forum /a/>>), ma le modalità e la struttura del forum parrebbe identica a quelle descritte sopra: ancora oggi, prima dell'accesso su uno qualunque dei forum presenti sul sito, si afferma che le tematiche possono vertere su <<contenuti adulti>>, nonché la necessaria accettazione delle <<regole>> presenti nella homepage.

[893]Parmy, Olson, *op. cit.,*pag. 39.

[894]*Ivi,* pagg. 48-49, identificano che già a quei tempi emergevano i c.d. <<*moralfag*>>, ossia gli utenti contestanti la depravazione del sito o che cercavano di mobilitarsi per fermare i contenuti illeciti del forum, ed esser bollati come tale risultava per il partecipante essere <<il peggior insulto possibile>>. Chiunque contestasse la moralità delle idee postate sul forum rischiava di diventare mirino degli insulti dell'intero forum ovvero- con la crescita di Anonymous – didiventare bersaglio delle attività di Anonymous: ecco perché per i partecipanti spesso conveniva aderire alla mentalità generale del gruppo. Per maggiori approfondimenti, si cita: Mc Alaney, *Are you anonymous? Social-psychological processes of hacking groups,* inMoustafa, *Cybersecurity and Cognitive Science*, 2022, Academic Press. (DOI:https://doi.org/10.1016/B978-0-323-90570-1.00003-6).

[895]Parmy, Olson, *op. cit.,*pag. 49.

[896]Un esempio, riportato da Parmy, Olson, *op. cit.,* pag. 65, è l'attacco eseguito contro Habbo Hotel il 12 luglio 2006.Prendendo come riferimento la notizia che in, un parco-divertimenti negli Stati Uniti, fu vietato a un bambino di due anni affetto da AIDS di immergersi in piscina, gli utenti si erano registrati sul sito, utilizzando come avatar un uomo con acconciatura afro, e avevano bloccato l'accesso alla piscina, dichiarando agli altri avatar che la stessa era<<chiusa perché piena di sfigati e ci si prende l'AIDS>>.

[897] Parmy, Olson, *op. cit.,* pag. 76, identifica il termine Lulz come <<una corruzione di LOL (live laughloud)>>, corrispondente al compiere scherzi e a ridere a spese e a danno di altri.

ufficiale della chiesa di Scientologynel 2008 (definito come <<progetto Chanology>>[898]), vista dall'associazione come un ente pericoloso in grado di ledere la libertà del pensiero .

Un'altra famosa operazione fu l'<<Operazione Payback>> nel 2011, una serie di attacchi DoS rivolta a un esteso quantitativo di siti che avevano negato il sostegno al sito WikiLeaks[899] (tra cui:Mastercard, Visa Paypal, Bank of America e Amazon), rendendoli inagibili per almeno un paio di giorni.

Nello stesso anno, bisogna segnalare anche gli attacchi eseguiti contro Barr, amministratore delegato della HBGary Federal(un'azienda di cyber security), che aveva affermato in un articolo di giornale di essersi infiltrato nell'associazione e di essersi messo in accordo con l'FBI per fornire loro le informazioni che aveva acquisito[900]: nel febbraio 2011 venne non solo bloccato e reso inagibile il sito dell'azienda, ma vennero anche pubblicate tutte le mail di Barr, pubblicato il suo indirizzo, pubblicate le foto scattate a lui ed eseguite chiamate minatorie a tutte le ore del giorno e della notte- proseguendo anche nelle settimane successive.

Citando altre operazioni avvenute globalmente nel corso degli anni: l'attacco nel 2012 contro circa 700 siti istituzionali israeliani come protesta contro l'esercito islamico[901]; la trafugazione e la pubblicazione di documenti informatici ufficiali del sito nel Ministero dell'Interno da parte di Anonymous Italia nel 2013[902]; gli attacchi nel 2015 contro siti terroristici islamici per vendicare le vittime di Charlie Hebdo e l'attacco contro il sito ufficiale per la prevendita dei biglietti dell'Expo; l'attacco contro siti ufficiali dei Comuni, Province e Regioni in Italia nel 2018 (c.d. <<Operazione Black Week>> [903]); la

---

[898]Parmy, Olson, *op. cit.,*pagg. 78-79 e ss., descrivono in dettaglio l'operazione. Si veda anche la pagina Wikipedia relativa al Progetto Chanology: https://it.wikipedia.org/wiki/Progetto_Chanology.

[899]Come riportato da: Parmy, Olson, *op. cit.,*pagg. 130-132, WikiLeaks era un sito che aveva acquisito- e successivamente passato a diversi giornali americani- oltre 250.000 messaggi interni tra le ambasciate americane, comprese informazioni importanti relative al governo statunitense. La scelta dei siti sovracitati di annullare le loro donazioni a sostegno del sito venne vista dal forum /b/ come un tentativo di censura dell'attività di WikiLeaks: di conseguenza era necessario per Anonymous vendicarsi, << in nome della libertà di parola>>.

[900] Per maggiori informazioni: Mann, T*hey're watching. And they can bring you down*, pubblicatosul FinancialTimes.com il 23/10/2011: https://www.ft.com/content/3645ac3c-e32b-11e0-bb55-00144feabdc0.

[901] Di Corinto, *Anonymous: "Abbiamo violato la rete jihadista*", pubblicato in LaRepubblica.it l'08/02/2015.https://www.repubblica.it/tecnologia/2015/02/08/news/anonymous_abbiamo_violato_la_rete_jihadista-106820821/; Mele,*La guerra di Anonymous all'Isis. Intervista ad Antonino Caffo,*pubblicato su Archivio di RaiNews.it il 24/12/2015https://www.rainews.it/archivio-rainews/articoli/guerra-di-Anonymous-Isis-Intervista-Antonino-Caffo-e41997f0-26f2-4638-b4f0-60e65337686e.html?refresh_ce.

[902] Argentieri, *Anonymous, hackerato Ministero dell'Interno*, pubblicato sul Corriere.it il 28/05/2013. https://www.corriere.it/cronache/13_maggio_28/anonymous-ministero-interno%20_0b9f2c86-c7c9-11e2-803a-93f4eea1f9ad.shtml.

[903] Di Corinto,*Anonymous Italia contro il governo: le università nel mirino degli hacker*, pubblicato su LaRepubblica.it il 29/10/2018.
https://www.repubblica.it/tecnologia/sicurezza/2018/10/29/news/anonymous_italia_contro_il_governo_le_universita_nel_mirino_degli_hacker-210320656/

pubblicazione delle e-mail certificate di oltre 30.000 avvocati italiani[904], e molte altre ancora. Quella più recente è stata la scelta nel 2022 di <<dichiarare guerra>> telematica alla Russia a sostegno dell'Ucraina[905].

Ora, da questa innumerevole serie di azioni che potrebbero anche essere ideologicamente condivise dalla popolazione, è sorto il dibattito sul fatto se gli <<Anon>>[906]debbano essere considerati degli <<eroi>> ovvero dei <<criminali>> [907]. Considerato quanto detto precedentemente nella sezione dedicata agli hacktivisti [908], il senso di onnipotenza derivante dalle loro abilità informatiche e la loro convinzione di poter agire contro ogni regola per il perseguimento dei propri ideali non possono esonerare i soggetti dalla responsabilità per aver violato ripetutamente la legge e causato danni economici e psicologici alle loro innumerevoli vittime.

Le sfumature dei diversi gruppi di Anonymous nel mondo sono tante e hanno tutte delle particolarità specifiche: nonostante la tematica politico-ideologica comune; il gruppo di Anonymous originario era spesso mosso da motivi di vendetta e non si faceva scrupoli a colpire soggetti sia privati che pubbliciin contrasto con la visione ideologica dei suoi membri o che si erano mostrati irrispettosi nei loro confronti. Il gruppo italiano, invece, parrebbe prediligerecome vittime delle proprie azioni le pubbliche istituzioni, le pubbliche autorità ovvero figure politiche o aziende nazionali,con scopo soprattutto di protesta a fine politico, ed è pronto a fare il possibile affinché venga assicurata la propria visione di giustizia e libertà[909].

Fatto questo quadro storico, si cercherà nel prosieguo della trattazione di comprendere più da vicino quali possono essere gli elementi di Anonymous riconducibili al fatto tipico dell'associazione a delinquere semplice.

---

[904] Porro, *Gli hacker di Anonymous pubblicano i dati di oltre 30mila avvocati (Raggi compresa)*,pubblicato su Wired.it il 07/05/2019, https://www.wired.it/internet/web/2019/05/07/avvocati-italia-luzsecita/ .

[905]Franceschini,*Anonymous e la guerra cibernetica in Ucraina. Domande e risposte per capire gli attacchi degli hacker*, pubblicato su LaRepubblica.it il 24/03/2022. https://www.repubblica.it/esteri/2022/03/24/news/anonymous_e_la_guerra_cibernetica_in_ucraina_domande_e_risposte_per_capire_gli_attacchi_degli_hacker-342704238/.

[906]In Bertram, *Authority and Hierarchy within Anonymous Internet Relay Chat Networks*, in *Journal of Terrorism Research*, 2015, Vol. 6 , Is. 3, (DOI: http://doi.org/10.15664/jtr.1089),

pag. 33, s' indica che <<Anon>> è il termine utilizzato dai membri di Anonymous per definirsi tali.

[907] Si veda: Volpicelli,D'Errico, *Anonymous, nuovi supereroi contro le forze del male?*, pubblicato su IlFattoQuotidiano.it l'11/01/2016. https://www.ilfattoquotidiano.it/2016/01/11/anonymous-nuovi-supereroi-contro-le-forze-del-male/2363875/ .

[908] Si richiama il paragrafo 1.1.

[909]Quanto detto finora emerge nell'articolo di: Mosca, *Anonymous Italia annuncia nuovi attacchi*, pubblicato su Wired.It il 29/10/2018 (https://www.wired.it/attualita/tech/2018/10/29/anonymous-italia-2018/), dove viene riportato l'incipit del video diffuso su Youtube da Anonymous Italia nel 2018 con cui elencano i siti italiani da loro violati: *<<C'è qualcosa di terribilmente marcio in questo paese, crudeltà e ingiustizia, intolleranza e oppressione* [...] *Se cercate il colpevole non c'è che da guardarsi allo specchio >>*.

Si è sinora tentato di descrivere chi siano questi soggetti componenti l'Organizzazionee quali siano le principali motivazioni che li spingono a commettere azioni illecite. Mancano però delle risposte a questioni basilari, ossia sul come agiscono e come si organizzano: bisognerà quindi partire dall'approfondire entrambe, al fine di comprendere meglio il loro funzionamento.

Solo dopo aver eseguito questi passaggi si potranno avere tutti gli strumenti necessari per cogliere appieno i principali ragionamenti della giurisprudenza italianaal fine consentire l'applicazione dell'art. 416 c.p. a queste.

4.1. Le modalità di attacco: il Denial of Service (cenni).

Il Denial-of-Service (<<Diniego di Servizio>> in italiano) corrisponde ad un numero importante di attacchi informatici di massa, consistenti nella <<contemporanea richiesta di comunicazioni esterne (*botnet*) operata da un numero elevato di individui, o da programmi>>[910], capaci di bloccare o rallentare gravemente il funzionamento di un sistema o di un programma informatico, impedendo definitivamente alla vittima di accedere ed utilizzarlo - nei casi più gravi, anche permanentemente.

Tuttavia, anche se l'attacco dura solo per un tempo limitato, la vittima non può dormire sonni tranquilli: oltre al fatto che tramite questi strumenti gli hacker hanno facile accesso a dati ed informazioni personali dell'utente[911] che possono in seguito esser rubati e poi venduti ovvero modificati, tramite il DoS è possibile riuscire a trovare eventuali falle nei software o programmi- bersaglio, rendendo dunque il sistema colpito facile preda futura di ulteriori attacchi per rubare informazioni e dati, nonché per future estorsioni online[912].
Gli attacchi sono spesso eseguiti anche in ambito imprenditoriale: secondo alcuni studi, il Denial of Service parrebbe essere la tipologia di mezzo più utilizzato anche a danno della proprietà industriale o intellettuale di aziende, allo scopo di ottenere segreti professionali ed eventualmente anche eseguirne la divulgazione a livello globale[913].

---

[910]Bussolati, *op. cit.,* pag. 263.
[911] Teichmann, Sergi, Wittmann, *The compliance implications of a cyberattack: a distributed denial of service (DDoS) attack explored*,in *International Cybersecurity Law Review*, pubblicato online il 2/06/2023.pagg.2-3. (DOI: https://doi.org/10.1365/s43439-023-00090-1). V. pure Musotto, Wall, *More Amazon than Mafia: analysing a DDoSstresserservice as organised cybercrime*,in *Trends in Organized Crime,* 2022, Vol. 25, Is. 2, pag. 177. (DOI: https://doi.org/10.1007/s12117-020-09397-5/).
[912]Musotto, Wall, *op. cit*., pag. 177.
[913]Teichmann, Sergi, Wittmann, *op. cit.,* pag. 3.

In questo quadro non sono da sottovalutare neanche i c.d. <<stresser>>, utenti dotati di elevate capacità informatiche che sono in grado di creare, monitorare e saper fermare una tipologia di attacco simile. Essi si trovano in una <<zona grigia>>[914]: possono agire a tutela degli utenti come anche essere direttamente ingaggiati per eseguire attacchi DoS contro i destinatari scelti dai loro committenti, e il quantitativo di denaro pagato è direttamente proporzionale alla qualità e alla potenza dell'attacco che verrà sferrato- nonché alla diminuzione della possibilità di frenarlo[915].

In aggiunta a tutto questo, per i sistemi <<ordinari>> è praticamente impossibile individuare preventivamente questi attacchi: sia perché gli attacchi hanno sempre strutture diverse tra loro, ma anche perché i diversi sistemi informatici e cibernetici non sono in grado di memorizzarle. Inoltre, seppur si potrebbe azzardare come soluzione a questa problematica l'incrocio dei dati memorizzati per ogni singolo attacco eseguito nel sistema cibernetico, di fatto non si hanno ancora strumenti informatici o cibernetici con una potenza tale da poter sopportare un carico così imponente di dati[916].

Questo quadro preoccupante per le vittime può comunque esser mitigato dal fatto che spesso queste tipologie di attacchi vengono anche utilizzate per testare il livello di sicurezza cibernetica di un sistema[917]: ciò però non toglie il numero enorme di vantaggi che l'autore di cybercrime può ottenere, causando danni enormi economici giuridici, psicologici e sociali ad un numero potenzialmente alto delle vittime (colpite non solo direttamente, ma anche indirettamente, considerando anche la presenza di ulteriori terzi usufruenti il programma o il sito della vittima).

Come accennato precedentemente, caratteristica basilare dello strumento è la sua variabilità in obiettivi, tempistiche, potenza e durata dell'attacco, facilitando gli hacktivisti nella imprevedibilità dei loro obiettivi e aumentando la possibilità che l'attacco abbia non solo successo, ma anche ottenga una reazione pubblica[918]. Ecco perché nel corso degli anni

[914]Musotto, Wall, *op. cit.*, pag. 179.
[915]*Ivi,* pagg.180-183.
[916]Javaheri, Gorgin, Lee, Masdari, *Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspective*, in *Information Sciences*, 2023, Vol. 626, pag.316. (DOI: https://doi.org/10.1016/j.ins.2023.01.067).
[917]Musotto, Wall, *op. cit.*, pag. 178.
[918]Si richiama il sottoparagrafo 1.1. precedente, dal quale risulta che gli hacktivisti, per quanto agiscano in anonimato, desiderino il più possibile ottenere un riconoscimento delle loro azioni dal resto della popolazione.

si è sviluppato un numero molto esteso di varianti del Denial of Service, di cui si farà un sommario esame dei tratti caratteristici di alcune tra le tipologie di DoS più famose.

La prima da cui si deve partire è senza dubbio il <<Distributed Denial of service>> (abbreviato come <<DDoS>>) [919] : si tratta della forma più comune ed utilizzata dall'Associazione Anonymous, consistente nell'attaccare il sistema-bersaglio con un'enorme quantità di dati. Due delle sue tipologie più comuni sono il <<Bandiwidth Distributed Denial of Service>>, dovel'obiettivo è quello di privare la vittima del traffico dati con cui navigare in rete, inviando dei *botnet*contenenti l'indirizzo IP della vittima falsificato (utilizzando la c.d. tecnica dell'<<IP Spoofing>>[920]), e il <<Reflection-based Distributed Denial of Service attacks>>, avente lo scopo di sovraccaricare la banda dati nel sistema, trasferendo in massa ulteriore traffico dati alla vittima lentamente, in modo tale che ella non si accorga di quanto sia successo se non al momento definitivo di diniego di accesso.

Un'altra tipologia da menzionare sono i <<Zero-DayDdoS Attacks>>[921], in grado di subentrare in un sistema-bersaglio ed esplorare attentamente il suo contenuto prima di attaccare una lacuna preventivamente individuata e studiata. Sono meno noti e meno frequenti del gruppo precedente, ma ben più pericolosi: sono infatti quasi impossibili da individuare – persino coi metodi scientifici e le tecnologie più avanzate a disposizione[922].

Infine, si deve accennare al <<Slow-rate Distributed Denial of Service attacks>>[923]: a differenza dei precedenti, in questo caso l'attacco consiste nell'utilizzo di una piccola <<zona>> di traffico dati con la quale superare facilmente gli eventuali sistemi di sicurezza attivi, e può essere attuata anche con l'utilizzo di un solo server. In questo modo, l'autore dell'attacco può facilmente creare dei *botnet*apparentemente innocui, attendere che si infiltrino nel sistema e far passare anche un lasso di tempo consistente tra quell'evento ed il momento dell'attacco definitivo.

Sulla base di quanto detto finora, parrebbe che gli Anon abbiano a disposizione degli strumenti invulnerabili per potere ottenere dati ed informazioni senza particolari sforzi. In

[919]Javaheri, Gorgin, Lee, Masdari,*op. cit*., pag. 320.
[920]Per ulteriori informazionisu questa tecnica, si rinvia alla pagina Wikipedia: https://it.wikipedia.org/wiki/IP_spoofing
[921]Javaheri, Gorgin, Lee, Masdari,*op. cit*., pag. 320.
[922]*Ibidem.*
[923] *Ibidem.*

realtà, il quadro finora presentato è incompleto: è necessario anche richiamare, in chiusura, le direzioni che la ricerca e la scienza stanno tentando di prendere per prevenire e frenare queste tipologie di attacchi, nonché precisare se le organizzazioni criminali online tendono ancora a proseguire la strada del DoS per la commissione dei reati o se invece si stanno manifestando nuove tendenze.

Riguardo la prima questione, purtroppo anche gli studi più recenti faticano nella creazione di un programma ovvero nell'individuazione di una metodologia informatica in grado d'identificare in tempo qualsiasi forma di attacco di Diniego di Servizio.

Un passo importante è stato compiuto col recente utilizzo della tecnologia AIper l'applicazione dei meccanismi informatici e scientifici a tale scopo, poiché essa si è rivelata esser molto utile per trovare eventuali anomalie rispetto al comportamento usuale dei sistemi. Tuttavia, essa non è in grado ancora di rilevare con certezza se quest'anomalia sia effettivamente di carattere sospetto ovvero sia normale, considerato anche l'enorme quantitativo di dati e informazioni in circolo in larga scala[924].

Si auspica dunque che vi sia in futuro una maggiore attenzione nello studiare e sperimentare diverse metodologie ingegneristiche, informatiche e scientifiche al fine di poter fornire una concreta ed efficace misura di difesa per le potenziali vittime.

Nel dettaglio, tra le diverse prospettive[925] suggerite come future possibili vie da percorrere per ricercatori, tecnici e studiosi,si menziona:

- L'utilizzo e sperimentazione di diverse metodologie devono tenere conto che gli attacchi sono tutti diversi tra loro: conseguentemente, è necessario sviluppare dei software con la capacità di sapersi confrontare con queste tecniche, senza fermarsi allo studio di una singola tipologia di attacchi e /o *modus operandi*;
- Lo sviluppo di apparecchiature e programmi in grado di elaborare controllare ed incrociare un'enorme quantitativo di dati provenienti dai diversi sistemi, in modo da facilitare il processo di ricerca;
- L'utilizzo di dati sempre aggiornati;
- La necessità di sperimentazione di diverse metodologie, specie se mai tenute precedentemente in considerazione da altri ricercatori.

È da segnalare, infine,che in tempi recentissimi gli attacchi informatici da parte di Anonymous parrebbero essersi dimezzati rispetto alla tendenza riscontrata in passato: la causa di questo parrebbero essere la presenza sia di idee conflittuali all'interno del gruppo

[924]Javaheri, Gorgin, Lee, Masdari,*op. cit*., pag. 335.
[925]*Ivi,* pag. 336.

che di <<falsi attivisti, che si sono infiltrati per danneggiare il collettivo e fare soldi alle sue spalle>>[926].

Questo non permette di conoscere esaustivamente se tutt'oggi il Denial of Service sia ancora il principale strumento utilizzato da Anonymous, ma forse questa diminuzione di tale tipologia di attacchi- dovuta anche all'avanzamento delle misure di sicurezza cibernetiche- potrebbe essere un segnale concreto della ricerca ovvero effettiva scoperta di nuovi strumenti informatici e/o cibernetici per la commissione delle loro attività illecite: saranno eventualmente il tempo e gli studi a trovare una risposta che dia conferma o smentisca quest'incertezza.

4.2. La struttura organizzativa: analisi dell'Internet Relay Chat Network.

Come accennato nel paragrafo precedente, l'organizzazione Anonymous si muove seguendo la struttura dello <<sciame>>, caratterizzato dall'assoluta assenza di gerarchia[927], dalla possibilità per gli utenti di poter facilmente accedervi ed uscire (spontaneamente o perché cacciati dagli altri utenti), nonché dall'interscambiabilità dei ruoli e delle funzioni tra i partecipanti.

In realtà, il quadro che è stato fornitoè di carattere approssimativo: la dinamica organizzativa tramite la quale i membri di Anonymous pianificano (prima in via generica, poi nel dettaglio) le proprie azioni illecite e si dividono i compiti necessari da svolgere per attuare le loro azioni è molto più complessa di quello che sembra.

Sarà dunque necessario analizzare quest'elemento ancora più nel dettaglio, partendo dallo strumento informatico in cui gli hacker (membri dell'organizzazione o in procinto di diventare tali) s'incontrano virtualmente: il canale Internet Relay Chat Network (in abbreviazione<<IRC>>) ed i suoi tratti principali di funzionamento.

L'IRC è un sistema molto diverso dalle comuni chat, blog o forum: infatti, non viene utilizzato da qualunque utente, ma soltanto da chi ha le conoscenze[928] ed i mezzi necessari per arrivare al suo accesso ed utilizzo[929].

---

[926] Porro, *Che fine hanno fatto gli hacker per una giusta causa*?, pubblicato su Wired.it il 06/06/2019, https://www.wired.it/internet/web/2019/06/06/hacker-attacco-anonymous/ .

[927] Ciò viene anche affermato direttamente dai membri di Anonymous stessi, in base anche da quanto riportato da Bertram, *op. cit.,* pag.16; Picarella, *op. cit*., pag. 330.

[928] Benjamin, Zhang, Nunamaker Jr., Chen, *Examining Hacker ParticipationLength in Cybercriminal Internet-Relay-Chat Communities*, in *Journal of Management Information Systems*, 2016, Vol. 33, Is.2, pag. 483, (DOI: 10.1080/07421222.2016.1205918) specificano che la conoscenza e le abilità in materia

In questa piattaforma, infatti, sussistono innumerevoli canali utilizzati per dialogare tra tanti soggetti in apposite "stanze"[930]e contemporaneamente consentire che il singolo veda in tempo reale i messaggi e commenti mandati da tutti i partecipanti in esse.

Vi sono in esso poi dei tratti peculiari,tali da non solo distinguerlo nettamente dai modelli <<ordinari>> dei forum di altre piattaforme del Web (es. *chat*), ma da renderlo ulteriormente oggetto di particolare interesse dagli studiosi [931]. Uno tra questi, in primo luogo, è l'assenza di strumenti di archiviazione dei messaggi: a differenza della stragrande maggioranza delle tipologie di messaggistica presenti nel Web, dove è possibile recuperare la cronologia delle conversazioni, nell'IRC non sussiste alcuno strumento – nemmeno di carattere automatico- in grado di archiviare le conversazioni per una successiva consultazione da parte degli utenti.
Altro aspetto fondamentale da segnalare è l'assenza di <<sottogruppi>> in base alle tematiche di discussione: la piattaforma è una sola ed in essa chiunque può parlare e dire quello che desidera nei diversi canali dell'IRC - arrivando, qualora egli fosse dotato di particolari capacità persuasive e di particolari <<riconoscimenti>> da parte degli altri membri[932], anche a influenzare il tono della discussione e l'oggetto della stessa;

Ultimo tratto particolare è il quantitativo di messaggi scambiati: tenendo conto che i membri passano gran parte delle loro giornate su queste chat[933], i messaggi che vengono scambiati al minuto arriva anche a sfiorare il migliaio- numero irraggiungibile con le stesse tempistiche da forum o chat presenti sul Clear Web.
Ogni utente, prima di accedere ad uno qualsiasi dei livelli (o stanze) della piattaforma, userà sempre nickname per mantenere l'anonimato, e riceverà un MOTD (<<Message of

---

tecnologico-informatica sono di livello variabile tra i partecipanti: ulteriore tratto su cui devono fare attenzione gli studiosi per individuare tra essi i veri cybercriminali.

[929] Secondo Benjamin, Zhang, Nunamaker Jr., Chen, *op. cit.*, a pag. 488, l'hacker dev'esser dotato in particolare d'un software abilitato per l'accesso a questa tipologia di piattaforma, poiché essa consentendo più dialoghi contemporanei tra gli utenti, comporta un quantitativo di dati ed informazioni da gestire nettamente superiore ad una chat o ad un forum. Nellostessosenso: Hudson, Witt, *Internet Relay Chat (IRC),* in AA.VV., *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications,* 2007, Volume 3, (a cura di) Bidgoli, John Wiley & Sons Ltd. (DOI: https://doi.org/10.1002/9781118256107.ch57), pagg. 890-891.

[930]Bussolati, *op. cit.,* pag. 264.

[931]Benjamin, Zhang , Nunamaker Jr., Chen, *op. cit*, pag. 488.

[932]In cosa consistano questi riconoscimenti se ne tratterà meglio in seguito, lungo questo punto.

[933]Paolillo, in *Language variation on Internet Relay Chat: A social network approach*, in *Journal of Sociolinguistics*, 2001, Vol.5 , Is.2, pag.185 (DOI: https://doi.org/10.1111/1467-9481.00147/), spiega che questo enorme quantitativo di ore passato sulla medesima piattaforma può esser equiparato ad un tentativo di <<socializzazione>> , in modo da creare e far consolidare <<i legami sociali>> in questi network, come avverrebbe in forma fisica. L'autore segnala però, che spesso questi utenti entrano ed escono nel corso della giornata, creando una sorta di sistema di rotazione del numero di utenti presente sulla piattaforma 24 h su 24. Nello stesso senso: Bertram, *op .cit*., pag. 17.

the Day>>) che gli darà alcune informazioni basilari fornite automaticamente sul server su quale è l'attività che sta avvenendo al momento nella piattaforma IRC (es. i nickname connessi, il tema di cui gli utenti stanno discutendo, ecc.).
Usando il codice <</list>>, gli utenti avranno una lista di tutte le stanze in quel momento attive, e potranno accedervi col codice <</join#channelname>>.
Aspetto interessante da tenere in considerazione è che la lista di stanze comprende solo quelle attive, poiché la loro creazione ed esistenza dipende dall'utilizzo di esse da parte degli utenti: ciò significa che anche il singolo utente può crearne una lui stesso e accedervi direttamente- anche se avente solo lui stesso come membro.

Bisogna fare una distinzione tra la tipologia di stanze presenti, perché si rivelerà essere un elemento chiave nella delineazione dell'elemento organizzativo dell'associazione Anonymous: alcune di esse sono private (c.d. <<stanze segrete>>), a cui possono accedere solo utenti prestabiliti al momento della creazione delle stanze stesse;altre - quelle con la denominazione #channelname vista sopra- sono pubbliche e qualunque utente da qualsiasi angolo del globopuò accedere ad esse. [934]

Quello che bisogna far notare è che questa piattaforma non viene unicamente utilizzata per scopi illeciti: essa viene utilizzata da un numero enorme di utenti con varie motivazioni, con consequenziale variabilità del numero di canali e di <<stanze>> contenute in essi, nonché mutevolezza dei contenuti di discussione in essa.
Perciò, una domanda che sorge immediatamente è quali possono essere gli elementi indicatori in grado di poter cogliere, tra le migliaia di stanze che si formano quotidianamente, quali siano quelle in cui i cybercriminali si riuniscono per pianificare le loro attività illecite.

Una prima strada che può essere seguita per rispondere a questa domanda è quella di studiare i diversi argomenti di discussione nelle diverse stanze: da ciò si è potuto notare come sia molto comune tra i cybercriminali discutere d'informazioni relative alle tecniche di hacking, cryptologia, creazioni di malwaree ai link per il diretto accesso al Black Market.
Questa via,a prima vista promettente, si è tuttavia rivelata nella pratica difficile da percorrere. Oltre al quantitativo delle discussioni e delle tematiche nelle diverse stanze (che, si ricorda, non possono esser in alcun modo archiviate), spesso gli utenti <<non-

[934] Tutte queste informazioni sull'accesso vengono riprese da: Hudson, Witt, *op. cit*., pag. 890.

cybercriminali>>trattano comunque di conoscenza informatica, senza mai tuttavia porre in essere l'attività di hacking (ad es. scambio d'informazioni sui codici di programmazione, sui sistemi operativi, ecc.)[935].Inoltre, è stato dimostrato[936] che non necessariamente la trattazione di contenuti tecnici o di mercato nero in un gruppo necessariamente comporta che esso sia composto da cybercriminali.
In definitiva, è piuttosto arduo individuare con certezza tra gli utenti chi siano effettivamente i cybercriminali solo tramite l'utilizzo di questo criterio.

Una seconda alternativa - indubbiamente più complessa e tortuosa, ma probabilmente avente più possibilità di successo- risulta essere l'analisi delle modalità d'interazione sociale e delle tipologie di relazioni che gli utenti intrecciano tra loro.
Infatti, affinché gli utenti possano esser considerati <<membri>> di queste comunità virtuali, essi debbono aver intrecciato una relazione virtuale con uno dei membri(più questo membro è apprezzato dalla comunità, meglio è): fino a quel momento, verranno trattati dei meri estranei nelle discussioni.
Un mezzo utile per la costruzione di questi legami <<d'amicizia>> è quella di scrivere messaggi diretti agli altri membri ovvero di chiedere loro l'amicizia sui social[937]: in questo modo, i membri possono partecipare più attivamente alle discussioni, ottenendo maggiore credibilità ed affidabilità agli occhi degli altri utenti[938].
Ecco dunque un primo dato fondamentale nell'elemento organizzativo dell'Organizzazione Anonymous (oltre l'assenza di gerarchia - già menzionata nel paragrafo precedente): dopo l'entrata in determinate <<stanze>> trattanti argomenti di carattere illecito, il rapporto sociale instaurato virtualmente con gli altri membri sancirebbe in via definitiva l'adesione dell'utente all'associazione a delinquere.

---

[935]Benjamin, Zhang, Nunamaker Jr., Chen, *op. cit*, pag. 502, fannoriferimento a: Holt, Kilger, *Know your enemy: The social dynamics of hacking*, cit., 2012, pagg.1-7, pubblicato su the HoneynetProject.org: https://www.honeynet.org/download/paper-know-your-enemy-the-social-dynamics-of-hacking/;Holt, Lampke,*Exploring stolen data markets online: products and market forces*, cit., in *Criminal Justice Studies: A Critical Journal of Crime, Law, and Society*, 2010, Vol.23, Is.1, pagg.33–50.(DOI: https://doi.org/10.1080/14786011003634415).Radianti, *A Study of a Social Behavior inside the Online Black Markets*., cit., in: AA.VV., *2010 Fourth International Conference on Emerging Security Information, Systems and Technologies*, IEEE, pagg.189-194. (DOI: DOI: 10.1109/SECURWARE17361.2010).
[936]Benjamin, Zhang, Nunamaker Jr., Chen, *op. cit*, pag. 501, citano come es. le discussioni di tecniche di hacking a scopo educativo.
[937]Bertram,*op .cit*., pag. 27, rivela infatti come per Anonymous il ruolo dei social media(in particolare, Facebook e Twitter) sia importante non solo a livello promozionale delle loro azioni, ma anche per instaurare legami più profondi con gli altri Anon.
[938] Benjamin, Zhang, Nunamaker Jr., Chen, *op. cit*, pag. 492. Altri fattori che possono influenzare l'affidabilità dell'Anon sono (Id., *op. cit*., pag. 495) l'anzianità come membro e la durata della partecipazione.

Ma non solo: sono le stesse interazioni sociali tra i partecipanti a determinare la nascita e la vita dell'associazione a delinquere stessa.

Approfondendo questo aspetto, si fa notare come anche l'intensità relazionale tra membri nello stesso canale IRC risulti variare e possa esser elemento di diversi indicatori.

Il primo aspetto è quello dell'intensità delle interazioni messaggistiche non solo tra membri nelle stesse stanze, ma anche tra membri di stanze diverse. Tramite quest'ultime, si riesce ad individuare nel canale dell'IRC la presenza di stanze di carattere centrale e a distinguerle daquelle di carattere invece più periferico[939].

È così possibile rilevare facilmente un aspetto molto interessante: emerge infatti che alcuni Anon – spesso presenti in queste stanze centrali- risultano ricevere molte più interazioni sociali rispetto ad altri membri[940].
Tramite quest'osservazione si riesce ad individuare una particolare figura di Anon, gli <<AnonOps>> (fusione dei termini <<Anon>> ed <<Operators>>): un nucleo ristretto di membri <<dotato di "privilegi amministrativi">>[941], intesi come capacità di gestione del canale e capacità di escludere gli Anon dalla partecipazione alle stanze, anche per <<violazione delle regole di comunicazione nel gruppo>>[942]. Gli AnonOps sono spesso o utenti tra i primi ad esser divenuti Anon in quel canale, ovvero lo sono divenuti in seguito ad apposito ed esplicito conferimento da parte di altri AnonOps- specie se riescono ad ottenere la loro attenzione tramite le loro capacità tecniche ovvero discorsive all'interno delle stanze[943].
Questo spigherebbe l'elevato numero di interazioni sociali rispetto agli altri, poiché gli Anon tenteranno di contattare gli AnonOps più spesso allo scopo di ottenere favori [944]ovvero nella speranza di arrivare loro stessi ad ottenere quegli stessi privilegi.

[939]Paolillo, *op. cit*., nelle pag. 197-198 identifica che, nell'analisi del canale IRC #india, le principali interazioni erano rivolte verso due gruppi (chiamati <<gruppo K>> e <<gruppo H>>), dalle quali si è dedotto che sono i gruppi principali. Invece, se le interazioni rivolte da parte degli Anon ad altri gruppi sono di livello minore, se ne desume che quegli stessi gruppi abbiano un ruolo di carattere più periferico.
[940]Bertram, *op. cit.,* pag. 22. Nello stesso senso: Paolillo, *op. cit*., pag. 188.
[941]Bussolati, *op. cit,* pag. 264.
[942]Paolillo, *op. cit.,* pag. 185.
[943]Secondo Olson, *op.cit.,* pag. 57, un classico esempio fu l'Anon<<Topiary>>, avente una grande capacità persuasiva e una forte personalità in grado di trascinare centinaia di membri nel compimento delle Operazioni(<< Per Topiary[…] quel ruolo era recitare>>).
[944]Paolillo, *op. cit.,* pag. 197.

Questo quadro permette di avere maggior completezza anche nello studio del linguaggio utilizzato nel canale IRC. Ad esempio, nel canale IRC #india parrebbe che la lingua prevalente (Hindi) utilizzata in esso sia necessaria per poter acquisire una posizione di rilievo nelle stanze: in particolare, se l'utente non ha particolari conoscenze della lingua e usa l'inglese[945], l'utilizzo di riferimenti socio-culturali e la presenza di relazioni forti può esser utilizzato al fine di acquisire una posizione maggiormente rispettabile rispetto alla moltitudine degli altri partecipanti.

Inoltre, l'utilizzo di linguaggio osceno- che dovrebbe rientrare nei divieti previsti dalle regole di comunicazione del gruppo- viene utilizzato più frequentemente tra membri delle stanze più centrali e pochissimo da quelle di carattere periferico (spesso occupate dai nuovi membri, i c.d. <<newbies>>), a dimostrazione di come anche lo stesso linguaggio possa essere una manifestazione del potere di cui sono dotati gli Operatori[946].

Tuttavia, non tutti gli AnonOps godono dei medesimi privilegi.

Considerando che vi sono diverse tipologie degli stessi[947] e che questeposizioni non sono fisse, in quanto possono esser sempre messe in dubbio dalla comunità[948], si giunge al secondo punto riguardante l'elemento organizzativo di Anonymous.

Nonostante il forte rifiuto dell'autorità da parte dell'intera Organizzazione,sulla base di quanto visto finora, si deve concludere che è necessariamente presente un livello minimo di struttura all'interno di Anonymous[949]. Tuttavia, non sussistendo gerarchia né figure apicali prestabilite,e allo stesso tempo dando a determinati Anon<<meritevoli>> la possibilità di acquisire dei privilegi all'interno del Canale IRC,la struttura organizzativa come elemento del fatto tipico assume dunque una connotazione nuova, in quanto perfettamente aderente ad un modello <<aperto>>e in costante mutevolezza come quello delle comunità virtuali.

Si parla infatti di un modello organizzativo:

---

[945] *Ivi,* pag. 202.

[946] *Ivi.,*pagg. 202-203.

[947] Bertram, *op. cit.,* pagg.18-19.

[948] *Ivi,*pag. 29, definisce infatti come questa leadership degli Operatori non sia mai di carattere <<fisso>>, quanto piuttosto sia collocata in <<un modello competitivo di risorse>>. Non bisogna poi tralasciare l'ulteriore fatto che il potere e l'influenza degli Operatori può sempre essere contestato – con fondate motivazioni- da parte degli altri Anon, che possono rivolgersi ad altri Operatori per la rimozione del privilegio.

[949] Si deve dunque seguire la linea di pensiero di Bertram, *op. cit.,* pag. 17, che richiama sul punto Melucci,*Challenging Codes: Collective Action in the Information Age,*cit., 1996, Cambridge University Press, pagg. 344-347 (DOI:10.1017/CBO9780511520891/), il quale si focalizza su <<la necessità di una forma minima d'organizzazione interna al fine di mantenere un'azione collettiva coesa>>. Nello stesso senso: Bussolati, *op. cit*., pag. 264;Paolillo, *op. cit.,*pag.209.

- a <<gerarchia orizzontale>>[950] : non c'è un capo che ripartisce i compiti e le funzioni tra i membri, ma tutti i membri decidono,di propria iniziativa, di ripartirsi le attività in base alle loro abilità e competenze ed eseguire le operazioni autonomamente;
- dotato di struttura flessibile;
- con il dato tecnologico <<assurto […] come elemento strutturale fondamentale>>[951], in quanto la Rete cibernetica è - nel caso specifico- strumento fondamentale per garantire la connessione tra utenti aventi la stessa ideologia politica e le medesime intenzioni criminali.

Nella specificità delle operazioni illecite eseguite da Anonymous, è stato tendenzialmente rilevato il seguente meccanismo[952]: di solito è un gruppo ristretto di Anon– aventi spesso un forte legame tra loro- che sviluppano l'idea di commettere l'operazione illecita alternativamente tramite messaggistica personale, ovvero nelle stanze pubbliche e private,ed organizzando nel dettaglio le operazioni in un'apposita stanza privata (definite in questo caso come <<stanze operazionali>>[953]), manifestando l'idea poi direttamente nelle stanze pubbliche, coinvolgendo il resto degli Anon come meri spettatori ovvero fornendo loro i dati definitivi per la partecipazione volontaria alle loro azioni su un piano più generale.

In chiusura, la metafora utilizzata per descrivere il rapporto tra gli AnonOps e l'insieme degli altri Anon presenti sul canale IRC è piuttosto calzante: viene infatti definito il loro rapporto come quello di un <<impresario ed il suo circo>>[954], dove gli Anon sono equivalenti a dei potenziali<<spettatori>>.Gli AnonOps- dotati spesso di lingua tagliente e provocatoria ovvero di elevate capacità tecniche ed informatiche- hanno il compito di attrarre con le loro doti gli spettatori inducendoli a partecipare direttamente al loro <<spettacolo>>. Più l'<<impresario>> presenterà uno spettacolo <<promettente>> in termini di divertimento ai suoi <<spettatori>>, maggiore sarà il pubblico che attirerà e che lo seguirà nella sua attività - anche se illecita.

---

[950]Picarella, *op. cit*., pag. 332.
[951]Bussolati, *op. cit,* pag. 267.
[952]V. sul punto quanto riporta Olson, *op. cit*., pag. 78 e ss., su come si sono svolte l'#OpPayback e #OpChanology; nonché le analisi compiute da Bertram,*op. cit*., nelle pagg.25-28, relativamente all'#OpGreenRights (una delle sezioni di Anonymous, che si occupa di eseguire attacchi informatici rivolti esclusivamente a sollevare l'attenzione sulla tematica ambientale. Si riporta qui il loro Blogspot: http://operationgreenrights.blogspot.com/) e alla #OpAustralia (una sezione di Anonymous rivolta localmente all'Australia e Nuova Zelanda).
[953]Bussolati, *op. cit,* pag. 264.
[954]Questa metafora la si ritrova in:Bertram, *op. cit*., pag. 29.

4.3.Il problema della configurabilità del delitto di associazione per delinquere ex art. 416 c.p., tra torsioni giurisprudenziali e istanze di riforma.

In base agli elementi emersi finora, si può intuire immediatamente come la giurisprudenza italiana,nei procedimenti penali contro i membri di <<Anonymous Italia>>, per la condanna per una serie di reati (nell'ordine: accesso abusivo a sistema informatici o telematici ex art. 615-*ter* c.p., danneggiamento di sistemi informatici o telematici ex art. 635-*bis*, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici ex art. 615-*quater* c.p.,interruzione illecita di comunicazioni informatiche o telematiche ex art. 617-*quater* c.p.), abbia avuto grosse difficoltà.

Infatti, si arriva finalmente alla domanda chiave di tutto quest'elaborato: come si dovrebbe inquadrare una fenomenologia esistente nello spazio cibernetico e ricondurla alla fattispecie a delinquere semplice ex. art. 416 c.p.?

Prima di enunciare quali sono stati i ragionamenti della Cassazione in proposito, bisogna fare questa breve premessa sui movimenti illeciti di Anonymous Italia, in modo da comprendere meglio i casi che si andranno ad analizzare in seguito.

Anonymous Italia utilizzavadue canali pubblici (uno destinato agli utenti internazionali, chiamato <<#Opitaly>>, l'altro a quelli italiani, definito <<#italy>>)dove si organizzavano gli attacchi Distributed Denial of Service, e due canali privati (denominati <<#phreedom>> e <<#hq>>), dove nel dettaglioun gruppo ristretto di utenti sceglievagli obiettivi, pianificava gli attacchi e formulavai testi con cui rivendicare la <<paternità>> dell'attacco. I siti bersaglio venivano scelti o in base all'attenzione mediatica del momento oppure in seguito a scansioni online, se all'esito delle stesse risultavano delle vulnerabilità nei siti stessi.

Riguardo il *modus operandi* del gruppo in questione, le tipologie degli attacchi informatici effettuati erano essenzialmente due: i già menzionati attacchi DDoS (eseguiti in seguito a reclutamento di utenti volontari sui canali pubblici), nonché gli accessi abusivi a sistemi informatici finalizzati a ottenere dati riservati – nello specifico, credenziali di accesso degli utenti edegli amministratori del sito per accedere alle aree riservate e per poter inviare, modificare o cancellare files.

Inoltre, in alcuni casi, si aggiungeva ulteriormente il *defacement* del sito, apparendo dunque nella homepage un messaggio di rivendicazione in linea con l'esaltazione della visione politico-ideologica secondo la quale gli hacker avevano agito.

Sul caso Anonymous si sono pronunciate due sentenze della Cassazione.

La prima è la sentenza della Sezione Feriale n. 46156 del 2013 relativa al rigetto di tutte le motivazioni del ricorso contro l'ordinanza del Tribunale del riesame di Roma, del 13 giugno 2013. Riguardo a quanto interessa in questa sede si menziona ilprimo dei due motivi di ricorso, ossia la violazione dell'art. 416 c.p. e vizio di motivazione per la mancanza di gravi indizi in ordine al reato summenzionato. Infatti, secondo la tesi della difesa:

- Vi è l'assoluta assenza nella fattispecie concreta di tutti e tre gli elementi del fatto tipico, in quanto il caso in questionenon costituirebbe un'associazione a delinquere, ma corrisponderebbe piuttosto a << uno spazio di libertà che si estende dalla tutela dei diritti umani e civili a quella dell'ambiente>>[955].
- Non sussisterebbe nemmeno la condotta di partecipazione dell'imputato, in quanto <<ciascun agente, sfruttando le proprie competenze tecniche, poteva agire autonomamente rispetto agli altri, senza neanche la consapevolezza del ruolo svolto da altre persone. >>[956].

La Corte di Cassazione ha negato la fondatezza delle motivazioni summenzionate riportate nel ricorso seguendo un lineare ragionamento.

Essa partì dal constatare che la struttura del gruppo si distribuiva in diverse attività (nell'ordine: <<la predisposizione del blog ufficiale dell'organizzazione e del video di propaganda>>; <<la predisposizione e gestione dei canali di comunicazione IRC privati>>; <<l'organizzazione, in tali canali, delle linee strategiche>>; <<la discussione sulla vulnerabilità dei siti da attaccare>>; << la definizione dei testi di rivendicazione poi diffusi mediante siti web>>; <<il mantenimento dei contatti con i media e con l'organizzazione>>, nonché anche con organizzazioni criminali estere): sulla base di tutti questi elementi, per la Suprema Corte non poteva esservi alcun tipo di dubbio sull'esistenza dell'elemento organizzativo e della sussistenza d'un organizzazione a delinquere, in gradodi perseguire stabilmente la commissione di reati informati. Conseguentemente, lo stesso imputato era riconducibile senza dubbio alla figura del partecipante ex art. 416 c.p., avendo lui stesso

[955]Cass.Pen. ,Sez.Fer., n. 46156 del 29/08/2013.
[956]Vedi nota di sopra.

mantenuto i contatti tra il gruppo e le organizzazioni internazionali, nonché ideato e partecipato alla realizzazione di numerosi attacchi online.

La seconda sentenza da analizzare è sempre della Sezione Feriale n. 50620 del2013[957], anch'essa emanata in seguito ad impugnazione dell'ordinanza del Tribunale di Roma emessa il 9/05/2013.
Il ricorrente ha pure qui dedotto l'erronea applicazione dell'art. 416, poiché ritenuti insussistenti sia il requisito oggettivo che quello soggettivo della fattispecie: il gruppo Anonymous Italia costituiva infatti un <<organizzazione volta a promuovere <<battaglie culturali ed ideologiche di notevole impatto […] sulle tematiche ambientalistiche e di difesa di libertà di espressione e di comunicazione del pensiero>>[958]; puntando dunque sulla <<illegittima criminalizzazione del dissenso politico-ideologico>>[959]

La Cassazione pure in questo caso ritenne l'infondatezza dei motivi di ricorso, eseguendo dei ragionamenti di cui vale la pena riportare qualche passaggio.
Il primo fu la considerazione dell'ammissibilità dell'applicazione dell'art. 416 c.p. in conformità alla precedente pronuncia del 2004 sulle associazioni a delinquere finalizzate allo scambio di materiale pedopornografico[960] anche nel caso di una <<comunità virtuale […], stabile ed organizzata>> operante solo in rete [961].
Facendo poi riferimento alla giurisprudenza in tema di terrorismo islamico, la Corte affermò come, in secondo luogo, il requisito del << "minimum" organizzativo>>[962]per la sussistenza dell'organizzazione può esser soddisfatto dalla struttura a <<cellule>>[963].

La Corte, da queste due argomentazioni, arriva alla conclusione che nel caso di specie l'aspetto rilevante è il <<programma condiviso anche in ordine alle modalità di perseguimento dei fini che il gruppo si propone>>[964]: conseguentemente, è perfettamente

[957]Cass. Pen., Sez. Fer., n. 50620/2013, in *Cass. Pen*., 2014, n.10, pagg.3307-3312.
[958]Cass. Pen., Sez. Fer., n. 50620/2013, pagg.3307.
[959]*Ibidem.*
[960]InCass. Pen., Sez. Fer., n. 50620/2013, pagg.3309, si fa esplicito riferimento a: Cass. pen., Sez. III, n. 8296/2004, in *Cass. pen*., 2006,Vol. 5, pag.1819.
[961]Si richiama a 1.3., in cui si è riportato come nella sentenza menzionata vi sia anche la ritenuta sussistenza dell'elemento soggettivo, consistente nella consapevolezza dei membri<<dello scopo e delle finalità del gruppo>>, assieme <<all'impegno di inviare periodicamente altre foto pedopornografiche>>.
[962]Cass. Pen., Sez. Fer., n. 50620/2013, pag.3311.
[963]In *Ibidem*, si precisa che questa struttura è dotata di <<estrema flessibilità interna, in grado di rimodularsi secondo le pratiche esigenze che, di volta in volta, si presentano>>.
[964]Cass. Pen., Sez. Fer., n. 50620/2013, in *Cass. Pen*., 2014, n.10,pag.3312.

ammissibile la configurazione di un programma criminoso avente ad oggetto l'accesso abusivoa sistemi informatici e telematici.
Tuttavia, nella parte finale della motivazione, viene sottolineato un aspetto interessante: la Corte non vuole e non ha mai voluto contestare la liceità di Anonymous a livello mondiale o degli scopi che persegue[965]; ma allo stesso tempo sottolinea come sia innegabile la compresenza in essa <<di cellule che possono avere pianificato iniziative illecite>>[966].

Ci sono diverse considerazioni da svolgere sui ragionamenti posti in queste due sentenze.

In primo luogo, bisogna partire dal riferimento alla sentenza relativa alle associazioni a delinquere volte alla produzione, distribuzione e diffusione del materiale pedopornografico: seppur sia stato eseguito il riferimento come elemento di dimostrazione dell'esistenza delle associazioni a delinquere su piani diversi dalla realtà fisica al fine di consentire la prosecuzione del ragionamento, è evidente che si presentano due realtà di associazioni a delinquere esclusivamente cibernetiche completamente diverse secondo diversi aspetti.

Una prima differenza evidente è sul piano organizzativo: nelle comunità pedopornografiche online la struttura è infatti fissa e ben chiara, vigono rigide disposizioni relative all'accesso e al mantenimento dello status di membro. Inoltre, in esse la distinzione tra partecipante e le forme di partecipazione qualificata (organizzazione, promozione, costituzione e direzione) è ben netta.
Invece, nel caso di Anonymous Italia si parlerebbe piuttosto di una <<comunità virtuale dotata d'elementi organizzativo-strutturali minimi>>[967], dove non solo la struttura è flessibile e non vi sono particolari controlli d'accesso per i nuovi membri, ma nella quale anche la presenza di ruoli apicali è categoricamente esclusa.
Non si dimentica in questo contesto il ruolo che può essere svolto dagli Operatori (assimilati alle figure del promotore/organizzatore[968]), ma bisogna sempre ricordare che è un ruolo che può esser messo in discussione dagli altri membricon la stessa facilità con cui si può ottenere: questo comporta l'assoluta instabilità di esso e la maggiore difficoltà d'inquadramento dell'utente come mero partecipante ovvero come promotore o organizzatore rispetto ai membridelle comunità pedopornografiche online.

[965]Nello stesso senso, Bussolati*, op. cit*., pag. 268.
[966]Cass. Pen., Sez. Fer., n. 50620/2013, in *Cass. Pen*., 2014, n.10,pag.3312.
[967]Bussolati, *op. cit.,* pag. 267.
[968]Cass.Pen. ,Sez.Fer., n. 46156 del 29/08/2013.

Un secondo aspetto riguarda il programma: se nelle associazioni a delinquere volte alla produzione, distribuzione e diffusione del materiale pedopornografico il programma non è solo scritto, ma anche ben delineato in ogni minimo dettaglio, nelle associazioni a delinquere cibernetiche finalizzate alla realizzazione di accessi abusivi a sistemi informatici, il programma criminoso parrebbe coincidere con la persecuzione in via illecita di un assetto ideale di valori: il programma, perciò, dev'esser <<condiviso anche in ordine alle modalità di perseguimento dei fini […] che il gruppo si propone>>[969] .

Un'ultima differenza, legata al vincolo associativo, risulta sussistere nel legame sociale: è aspetto indubbio che sia carattere comune delle associazioni a delinquere esclusivamente cibernetichela presenza di legami forti tra i membri[970], tuttavia, mentre le associazioni a delinquere pedopornografiche sono regolate da rapporti basati su <<meccanismi di reciprocità>> (nello specifico, lo scambio di informazioni e consigli sul tema della pedofilia); in Anonymous Italia, invece, emergerebbe come preponderante il senso di appartenenza al gruppo-aspetto emergente dalle costanti rivendicazioni degli attacchi informatici del gruppo da parte degli stessi membri.

Il secondo aspetto da analizzare è invece il richiamo alla materia del terrorismo.
È invero palese che il richiamo alle <<cellule>> - proprie della struttura organizzativa delle associazioni terroristiche di matrice islamica - sia rivolto al solo scopo di affermare la generale liceità del canale e di focalizzare l'attenzione solo sul <<secondo livello>>[971] del canale IRC (costituito dalle camere operazionali). Tuttavia, questo rinvio può risultare pericoloso, poiché realizzerebbe l'errore di far coincidere l'ideologia politica con il programma criminoso (analogamente a quanto accade per le organizzazioni con finalità terroristiche, nelle quali il <<comune progetto politico-militare>> corrisponde sia <<all'*affectio societatis*>> che <<allo scopo comune del <<sodalizio>> terroristico>>[972]).

[969]Secondo Cass. Pen., Sez. Fer., n. 50620/2013, in *Cass. Pen*., 2014, n.10, pagg.3310.
[970]In base agli studi condotti da: Wellman, Salaff, Dimitrova, Garton, Gulia, Haytornthwaite, *Computer Networks as Social Networks: Collaborative Work, Telework, and Virtual Community*, in *Annual Review of Sociology*, 1996, Vol. 22, Is. 1, pag. 224. (DOI: 10.1146/annurev.soc.22.1.213Picarella, *op. cit.,* pag. 384, se ne trae che l'intensità di questi legami- maggiore rispetto a quella presente tra membri di un'associazione a delinquere presente unitamente nel mondo fisico- è dovuta al fatto che i partecipanti si incontrano in piattaforme online dove possono esplorare interessi comuni.
[971]Secondo Cass. Pen., Sez. Fer., n. 50620/2013, cit., pag. 3308.
[972]Bussolati, *op. cit*., pagg. 269-270.

Se infatti si seguisse quest'approccio, oltre al possibile rischio di arrivare a paragonare la fattispecie associativa all'ideologia terroristica, si potrebbe arrivare pure a far corrispondere l'insieme dei valori ideologici, politici e sociali come programma criminoso. Come però si è detto più volte nel corso di questo capitolo, non necessariamente gli hacker si riuniscono ed organizzano per il compimento di finalità illecite, ma vi sono molti casi in cui i gruppi di utenti si riuniscono per discutere, decidere e poi compiere attività pienamente lecite: arrivare a far corrispondere il programma criminoso all'assetto ideologico- politico degli utenti comporterebbe dunque la penalizzazione anche ad ipotesi di associazioni esclusivamente cibernetiche di carattere lecito, violando palesemente la libertà di associazione ex art. 17 della Costituzione e del principio di personalità della responsabilità personale ex art. 27 della Costituzione.

Rimangono tuttavia dubbi e critiche da muovere contro entrambe le pronunce esaminate.
Innanzitutto, bisogna partire dall'incriminazione dei soli partecipanti alle stanze private (dove, si ricorda, vengono pianificate nel dettaglio le operazioni illecite da compiere, ma spesso l'idea di formazione di una <<clique>> illecita avviene nelle stanze principali).
Dalle pronunce esaminate, parrebbe che la giurisprudenza definisca i canali come <<contenitore del programma criminoso generale>> [973] in quanto antecedenti al perfezionamento delle operazioni illecite nelle stanze operazionali, ma questa risulta essere una percezione errata.
Perciò, l'indicazione della generale liceità dell'Associazione Anonymous è corretta, ma non sufficiente: sarebbe necessario spiegare nel dettaglio questa sua caratteristica, in modo tale da far comprendere che non tutti gli hacker siano <<eroi>>, ma neanche che essi debbano esser considerati necessariamente dei criminali in quanto membri di Anonymous.

Altro aspetto interessante da far notare risulta essere la vaghezza con cui ancora viene delineata la struttura organizzativa tra i diversi livelli e stanze, nonché la difficoltà di <<rilevare i confini associativi>>[974].

Vi è inoltre da segnalare il potenziale rischio di confusione dell'elemento organizzativo nelle associazioni a delinquere esclusivamente online, poiché la piattaforma online è contemporaneamente strumento di comunicazione,spazio di interazione e elemento

[973]Bussolati, *op. cit*., pagg. 269.

organizzativo: come si è potuto notare da un breve confronto tra le comunità online di Anonymous e quelle pedopornografiche, l'organizzazione parrebbe strettamente legata alla piattaforma digitale in cui essa sorge e si sviluppa- conseguentemente, è necessario verificare la sussistenza dell'elemento organizzativo caso per caso.
Infine, rimane un dubbio relativamente all'aspetto della condotta di partecipazione, sulla quale la giurisprudenza ancora non si è pronunciata: il membro delle stanze generali che un'unica volta decide di aderire ad un'attività illecita, supponendo che venga individuato, dovrebbe esser condannato come concorrente esterno ex art. 110 ovvero si tratta sempre di condotta di partecipazione ex art. 416 c.p.?

In definitiva, parrebbe che l'astrattezza degli elementi della fattispecie ex art. 416 c.p. si ritrovi oggi a fare i conti con dinamiche, caratteristiche e metodologie completamente diverse da quelle che avvengono nel mondo fisico, ma pur sempre in grado di poter potenzialmente offendere o mettere in pericolo l'ordine pubblico.

Si deve perciò chiudere con una domanda espressa più di vent'anni fa, ma che comunque non ha perso la sua attualità: <<il diritto sarà in grado di affrontare tali cambiamenti ed elaborare regole che non risultino in perenne conflitto con la realtà sociale?>>[975].
In base a quanto detto finora sulle associazioni a delinquere esclusivamente cibernetiche, è evidente che ancora non si è trovata una risposta definitiva.
Le alternative rimangono dunque due: restare ancorati al mondo fisico come unico parametro di riferimento ma fare fatica nel ricondurre (quando possibile) ad esso atti illeciti avvenuti nel mondo virtuale, oppure elaborare disposizioni penali *ad hoc* specificamente riferite ad uno spazio in costante mutamento come quello cibernetico.

Posto che (come si è visto in questo capitolo) la prima via è stata ampiamente percorsa ma ha fatto emergere problematiche ed incertezze interpretative, forse converrebbe che il Legislatore si orientasse per la seconda opzione: probabilmente più complessa e tortuosa della prima, considerata la costante mutevolezza dello spazio cibernetico, maforse in grado di fornire una tutela più efficace ed estesaal bene giuridico.

[975]Maggipinto, *Reati nella Rete, tutti i nodi da sciogliere. Se il cybercrime mette in crisi il Codice*, in *Dir & Giustizia*, 2006, vol.6, pag. 61.

Conclusioni

Con questo elaborato si è cercato di svolgere una disamina delle principali criticità che connotano la fattispecie di associazione per delinquere semplice *ex* art. 416 c.p., anche in relazione alle più recenti conformazioni che la stessa assume nel c.d. cyberspazio.

La scelta del Legislatore del 1930di prevedere una fattispecie penale descritta con terminologia generica e ampia, al fine di poterne consentire l'applicabilità anche alle forme di associazione a delinquere semplice che si sarebbero manifestate in futuro, è stata indubbiamente una mossa vincente, visto che l'articolo 416 c.p. che punisce, appunto, coloro (almeno tre persone) che si associno allo scopo di commettere più delitti-trova tuttora ampia applicazione nella prassi.

Tuttavia, l'eccessiva astrattezza degli elementi costitutivi della figura di reato (nonché l'inafferrabilità del bene giuridico dell'ordine pubblico, del quale si fa fatica a trovare un riferimento empiricamente percepibile), la prevalenza assoluta dell'elemento dell'organizzazione rispetto agli altri due elementi del fatto tipico(ossia il vincolo associativo e il programma delittuoso)- tale da crearne quasi il loro subordinamento-, nonché la difficoltà d'individuare la soglia di rilevanza penale della condotta di partecipazione,hanno permesso di cogliere come questa fattispecie sia rimasta, paradossalmente,ancorata ad un tempo e a delle dinamiche non più rispondenti al nostro presente.

Peraltro verso, la vaghezza del concetto di associazione e la genericità nella descrizione degli elementi costitutivi della stessa si riverberano sulla difficoltà che la giurisprudenza incontra nel ricondurre, spesso con esiti tra loro contrastanti, i diversi casi specifici alla fattispecie in esame (specie con riguardo all'individuazione degli estremi della condotta di partecipazione, rispetto alla quale si oscilla tra l'accoglimento del criterio causale, di quello dell'inserimento organico o, ancora, del criterio c.d. misto). Infatti, si è potuto ben notare come il panorama giurisprudenziale in materia sia molto frammentario e mutevole .Questa confusione -sia della dottrina che della giurisprudenza – ha, tra l'altro, contribuito a rendere desueta tra i cittadini la percezione dell'esistenza di altre realtà diverse dall'associazione mafiosa, così come della loro evoluzione in forme altrettanto temibili e preoccupanti.

Bisogna perciò unirsi al coro degli studiosi che demanda un'urgente revisione della fattispecie. Sarebbe peraltro necessario considerare tutti gli elementi che compongono la

fattispecie, senza privilegiarne alcuni piuttosto che altri, per poter eventualmente formulare un'ipotesi di riforma: questo non solo eviterebbe il rischio di passare dall'attualizzazione della fattispecie allo stravolgimento del significato e della portata della stessa, ma anche sarebbe in grado di garantire un auspicabile riavvicinamento della norma penale al principio di tassatività, attraverso l'elaborazione di una fattispecie penale dai contorni ben definiti, in grado di punire le diverse tipologie di associazione che si affacciano (e si affacceranno in futuro) nel panorama nazionale e transnazionale.

Rispetto invece alle proposte d'introdurre nel Codice Penale più fattispecie penali di associazione a delinquere semplice, corrispondenti a fenomeni meritevoli di una risposta penale, a mio parere bisogna pronunciarsi negativamente: la presenza di diverse fattispecie di associazione a delinquere semplici comporterebbe il rischio d'una eccessiva frammentazione del sistema di risposta al reato associativo,perdendo al contempo l'elasticità che, seppur bisognosa di correttivi,consente comunque all'art. 416 c.p. di trovare applicazione rispetto a nuove forme di associazione a delinquere.

Passando poi all'analisi delle dinamiche del sistema cibernetico e della legislazione italiana e sovranazionale sull'argomento,si è avuta una piena conferma di come sia necessario uno studio trasversale e interdisciplinare(in particolare, delle materie tecnologiche,economiche, sociologiche, psicologiche e criminologiche), al fine di capire meglio come il diritto possa mantenere la propria efficacia nel regolare la moltitudine di rapporti pubblici e privati secondo i nuovi ritmi e meccanismi propri del mondo cibernetico (ricordando, ad esempio, le caratteristiche dell'anonimato, la velocità di creazione, modificazione ed estinzione dei rapporti sociali, l'aspetto della << aterritorialità >> della Rete, ecc.), a piena dimostrazione di come il mondo virtuale ormai sia compresente alla realtà fisica dell'Uomo.

In riferimento alla tematica del cybercrime, l'approccio summenzionato è fondamentale per il penalista, perché fornisce ulteriori strumenti di lettura per comprendere meglio nuove forme di reati cibernetici, quali possono essere le possibili varianti ed evoluzioni tecnologiche di tradizionali tipologie di reato,nonché quali misure giuridiche ed informatiche si rivelerebbero essere le più adatte per poterli prevenire e perseguire penalmente in via più efficace.

Questo è stato reso evidente dall'analisi di due diversi profili del tema in questione.

Il primo è stato, senza alcuna ombra di dubbio, l'analisi innanzitutto della legge italiana n. 48 del 2008 in ratificazione della Convenzione Cybercrime del Consiglio d'Europa del

2001, con cui il Legislatore, in tutta fretta, ha posto in essere un atto legislativo per la disciplina di una realtà non più rispondente ai parametri di qualsiasi reato tradizionale (caso esemplare è stata la frode informatica).

Non si intende qui contestare la scelta del Legislatore italiano d'inserire le singole fattispecie di reato nel codice penale configurandole sul modello di fattispecie penali preesistenti, e non in una Sezione *ad hoc*, in modo da tener conto anche della diversità e della peculiarità del bene giuridico meritevole di tutela,tuttavia è necessario imputare al Legislatore Italiano la poca cura nella formulazione di fattispecie criminose non rispondenti pienamente alle dinamiche del sistema cibernetico, portando, come risultato, una tutela soltanto parziale per i cittadini italiani contro i reati consumatisi in esso.

È di tutta evidenza, infatti, che quello dei *cybercrimes* è un ambito estremamente complesso, al quale vengono ricondotte tipologie di reato molto diverse l'una dall'altra: sia fattispecie che presentano, all'interno della definizione normativa, elementi tipici descrittivi di modalità, oggetti, attività frutto della tecnologia informatica e contengono almeno un elemento essenziale o circostanziale, volto a richiamare espressamente la Rete (reati informatici e cibernetici in senso stretto), sia reati tradizionali, che benché non presentino elementi tipici caratterizzati dalla tecnologia, possono essere applicati a fatti commessi tramite quest'ultima (reati informatici e cibernetici in senso lato).Si tratta quindi di un settore che richiederebbe un serio ripensamento da parte del legislatore.

Il secondo è stato l'analisi dei profili criminologici e psicologici generali degli autori e delle vittime dei reati cibernetici (con particolare attenzione alla figura dell'hacker): forse è stata la parte che in tutto questo percorso ha comportato maggiore lavoro, ma senza di essa non sarebbe stato possibile cogliere appieno,non solo il funzionamento del sistema cibernetico, ma anche l'atteggiarsi della criminalità nel cyberspazio, individuando aspetti che si sono rivelati fondamentali nella trattazione dedicata alle associazioni a delinquere esclusivamente cibernetiche – *in primis*, il "machiavellismo" ed il senso di onnipotenza dell'autore di reato cibernetico, dovuto anche alle basse possibilità di esser individuato ed in seguito penalmente perseguito.

Facendo infine una doverosa parentesi sul panorama sovranazionale, sulla base delle ricerche svolte è necessario segnalare la presenza di due problematiche diverse: da un lato, vi è questo costante tiro alla fune tra la previsione di norme generali, se non generiche (tali da garantire l'adattabilità nei vari Stati) e l'esigenza di conferire specificità alle diverse condotte penalmente perseguibili; dall'altro, vi è l'emersione – specie nelle trattative ONU che si stanno svolgendo in questo periodo, dirette all'adozione di una nuova Convenzione

sul cybercrime – dell'interesse dei vari Stati a far prevalere la propria visione di sistema di contrasto ai reati cibernetici piuttosto che propendere per la collaborazione e la mediazione al fine di arrivare ad una Convenzione unitaria in grado di armonizzare a livello mondiale il sistema di risposta al cybercrime(che è, per sua natura, transnazionale), e ciò benché sia nota globalmente la tendenza di crescita dei reati cibernetici (specie dopo la pandemia mondiale degli ultimi anni).

Riprendendo i vari profili problematici emersi nel lavoro anche nella trattazione finale dell'associazione a delinquere online, con specifico riferimento al caso Anonymous, si è notato come, curiosamente, in questa situazione sembrerebbe quasi rovesciarsi la situazione riscontrata rispetto al fatto tipico con riguardo all'associazione per delinquere operante nella realtà fisica: nel cyberspazio è il dato organizzativo ad assumere un ruolo quasi secondario rispetto ai legami sociali dei membri e alle motivazioni ideologiche da perseguire con finalità illecite.

Tuttavia, il confronto con le comunità online pedopornografiche ha permesso di capire non solo che si tratta di un fattore proprio di questa tipologia di associazione a delinquere, ma anche che in realtà il fatto tipico di queste associazioni criminose esclusivamente cibernetiche è spesso determinato dalle piattaforme di rete in cui questi gruppi illeciti si formano, le cui regole (più o meno rigide) relative all'accesso e al mantenimento dello *status* di membro, così come la più o meno ampia flessibilità dei ruoli, incidono sulla conformazione del sodalizio criminoso.

Si è riscontrato, ad esempio, che l'organizzazione Anonymous si muove seguendo la struttura dello <<sciame>>, caratterizzato dall'assoluta assenza di gerarchia, dalla possibilità per gli utenti di poter facilmente accedervi ed uscire, nonché dall'interscambiabilità dei ruoli e delle funzioni tra i partecipanti; si è inoltre visto come la dinamica organizzativa tramite la quale i membri di Anonymous pianificano (prima in via generica, poi nel dettaglio) le proprie azioni illecite e si dividono tra loro i compiti necessari per attuarle è molto complessa ed opera attraverso la piattaforma Internet Relay Chat Network e le innumerevoli "stanze" di cui essa si compone.

Un punto interessante da far cogliere è stato lo scoprire che le attività e le condotte poste in essere online dalle associazioni c.d. "hacktiviste"non sempre sono in tutto e per tutto di carattere illecito – e dunque, perseguibili penalmente: se il gruppo si muove lecitamente o meno tutto dipende dalle circostanze del caso specifico. Questo comporta un ulteriore ostacolo per il giurista, che è tenuto alla ricerca di nuovi criteri in grado di evitare che la

repressione penale del fenomeno associativo si estenda a fenomeni leciti - come ha avuto modo di precisare la giurisprudenza italiana con riguardo all'Associazione Anonymous in generale.

Vi è comunque la necessità di un doveroso ripensamento dell'impostazione giurisprudenziale riguardo alla configurabilità del fatto tipico e della condotta di partecipazione rispetto a queste tipologie di associazioni a delinquere online.

Nello specifico, il focalizzarsi (come si è fatto nelle sentenze rese nel caso Anonymous Italia)solo sui partecipanti nelle <<stanze operazionali>> e non anche sui soggetti che aderiscono alla fase finale dell'attività illecita (ossia, la presentazione della data ed ora dell'operazione) parrebbe un approccio eccessivamente semplicistico: è necessario chiedersi se non solo chi organizza l'operazione, ma anche gli utenti aderenti alla singola operazione illecita (pure pochi secondi prima dell'orario programmato per il suo compimento) debbano esser considerati allo stesso modo partecipanti ex art. 416 c.p. ovvero si configurino piuttosto come concorrenti esterni ex art. 110 c.p. richiamando alla memoria quanto il confine tra partecipazione e concorrente esterno sia di carattere piuttosto labile, come visto in questo lavoro.

In definitiva, è necessario predisporre una nuova normativa penale rivolta specificamente alle associazioni a delinquere operanti esclusivamente online oppure no? Vi sono pareri contrastanti sul punto, sul quale ancora non si è trovata una risposta univoca. Vista la diversità delle dinamiche del mondo cibernetico, sarei portata ad affermare la necessità di un'apposita disciplina normativa relativa ai i reati che si consumano, in forma associativa, in questa dimensione.

Tuttavia, tenendo conto della struttura elastica dell'art. 416 c.p., potrebbe essere sufficiente predisporre nell'articolo stesso un apposito riferimento alle associazioni a delinquere online, individuandone eventuali elementi specializzanti aggiuntivi, piuttosto della creazione di una norma *ad hoc*.

Quanto detto rimane però solo una mera riflessione: è tuttavia auspicabile che dottrina e giurisprudenza, e, soprattutto, il Legislatore italiano ricerchino una risposta conforme all'ordinamento penale ma allo stesso tempo che tenga conto delle caratteristiche peculiari del mondo virtuale, rispetto ad un fenomeno comunque in grado di suscitare allarme sociale e di mettere in pericolo l'ordine pubblico.

Un ultimo appunto da svolgere è poi rivolto alle associazioni a delinquere online ibride, ossia le organizzazioni criminali finalizzate sia alla commissione di reati cibernetici, sia alla commissione di reati "tradizionali" nella realtà fisica: se è emerso che gli studi su quelle esclusivamente cibernetiche sono di carattere recente ma tuttora carenti, ho rilevato che gli studi sulle prime sono ancora più ridotti di numero: queste altre realtà,anch'esse presenti e di uguale importanza, meriterebbero invece adeguata attenzione, considerata la maggiore potenzialità lesiva del bene giuridico tutelato che le connota.

Bibliografia

AA.VV., *Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, Atti Congresso UNODOC Salvador (Brasile) 12-19aprile 2010, https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf .

ACCILI SABBATINI M. A., *La Convenzione di Palermo ed i negoziati per il rafforzamento della cooperazione internazionale*, in Rivista di Studi e Ricerche contro la Criminalità Organizzata, vol. 5, num. 4, 2019, pagg. 29-53 (DOI: http://dx.doi.org/10.13130/cross-13095/).

AHMAD A., WEBB J., DESOUZA K. C., BOORMAN J., *Strategically motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack*, in *Computer Security,* Vol. 86,2019, pagg.402– 418.

ALEO S., *Sistema Penale e criminalità organizzata. Le figure delittuose associative*, Giuffrè, 1999.

ALMOMANI A., *Darknet traffic analysis, and classifcation system based on modified stacking ensemble learning algorithm,*in *Information Systems and e-Business Management,* 2023 (DOI: https://doi.org/10.1007/s10257-023-00626-2).

ANGIONI F., *Condizioni di punibilità e principio di colpevolezza*, in *Rivista Italiana di Diritto e Procedura Penale*, 1989, pag.1440 e ss.

ANTONINI E., *Le associazioni per delinquere nella legge penale italiana,* in *La Giustizia Penale,* parte II,1985, pp. 286-319

APRUZZESE A., *Autori e vittime nella criminalità informatica,* in *Rivista Quadrimestrale di Criminologia, Vittimologia e Sicurezza*,Vol. 3 e 4, numeri 3 e 1, 2009/2010, pagg. 101-106.

ARGENTIERI B., *Anonymous, hackerato Ministero dell'Interno*, pubblicato sul Corriere.it il 28/05/2013. (https://www.corriere.it/cronache/13_maggio_28/anonymous-ministero-interno%20_0b9f2c86-c7c9-11e2-803a-93f4eea1f9ad.shtml/).

BALDESSARELLI F.,*A proposito della rilevanza giuridica della distinzione tra "res corporales" e "res incorporales" nel diritto romano classico*, in *Revue internationale des droits de l'antiquité*, Vol.XXXVII, 1990, pagg. 71-116.

BALLONI A., et al., *Criminologia Applicata*, CEDAM, 2019.

BALSAMO A.,MATTARELLA A., TARTAGLIA R., *La Convenzione di Palermo: il futuro della lotta della criminalità organizzata transazionale,* Giappichelli Editore,2020.

BARILE P., voce *Associazione (diritto di),* in *Enciclopedia del Diritto*, Vol. III, Giuffrè, 1958.

BASSOLI E.,*Diritto di Internet. I crimini informatici, il dark web e le web room (vol. II)*, Pacini Editore, 2021.

BENJAMIN V., ZHANG B., NUNAMAKER Jr., CHEN H., *Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities,* in *Journal of Management Information Systems*, Volume 33, Issue 2,2016, pagg. 482-510 (DOI: 10.1080/07421222.2016.1205918).

BERNARDI A., *La competenza penale accessoria dell'Unione europea: problemi e prospettive,* in *Diritto penale contemporaneo– Rivista Trimestrale*., 2012, pag. 21 ss.

BERTOROTTA F., *Concorso eventuale di presone e reati associativi*, in *Rivista Italiana di Diritto e Procedura penale*, fasc.4, 1998, pagg. 1273 - 1309.

BERTRAM S. K., *Authority and Hierarchy within Anonymous Internet Relay Chat Networks*, in *Journal of Terrorism Research*, Volume 6, Issue 3, 2015, pagg. 15-34, (DOI: http://doi.org/10.15664/jtr.1089).

BIDGOLI H., *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications*, Volume 3, John Wiley & Sons, Inc., 2007 (DOI: https://doi.org/10.1002/9781118256107.ch57).

BONAVITA S., CORTINA A., STRINGHI E., *"Conosci il tuo nemico": un primo approccio tassonomico ai principali attacchi informatici nel settore del cybercrime bancario e finanziario*, in *Ciberspazio e Diritto*, vol.21, n.66, (3-2020), pagg.451-488.

BORRUSO R., voce *Informatica giuridica,* in *Enciclopedia del Diritto*, Giuffrè, 1997.

BOSCARELLI F.,voce *Associazione per delinquere*, in *Enciclopedia del Diritto*, Vol. III, Giuffrè, 1958.

BOSSLER A., HOLT T. J., 2010. The Effect of Self-Control on Victimization in the Cyberworld. *Journal of Criminal Justice*, vol. 38, Issue 3, pagg. 227-236 (DOI: 10.1016/j.jcrimjus.2010.03.001/).

BRICOLA F., (voce)*Punibilità (condizioni obiettive di)*, in *Novissimo Digesto Italiano,* vol. XIV, UTET, 1967.

BRICOLA F., *Considerazioni esegetiche sul dolo specifico del reato di falso in scrittura privata,* in *Archivio Penale*, vol.II, 1960, pag.65.

BRIGHI R.,DI TANO F., *Identità, anonimato e condotte antisociali in Rete. Riflessioni informatico-giuridiche*, in *Rivista di filosofia del diritto, Journal of Legal Philosophy*, 2019, pp. 183-204, (DOI: 10.4477/93373).

BROADHURST R., ALAZAB M., CHON S., *Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime,* in *International Journal of Cyber Criminology,* Volume 8, Issue 1,2014, pag. 3. (DOI:https://ssrn.com/abstract=2461983).

BUNCH J., CLAY-WARNER J., LEI M. K.*, Demographic characteristics and victimization risk: Testing the mediating effects of routine activities,*in*Crime & Delinquency*, Volume 61, Issue 9, 2015,pagg.1181-1205, (DOI:https://doi.org/10.1177/0011128712466932).

BURCHER M., WHELAN C., *Social network analysis as a tool for criminal intelligence: understanding its potential from the perspectives of intelligence analysts*, in *Trends in Organized Crime*, Volume 21, Issue .3,2018, pagg. 278-294. (DOI: https://doi.org/10.1007/s12117-017-9313-8).

BURTON A.,COOPER C., DAR A., MATHEWS L., TRIPATHI, K., *Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review,*in *Experimental Gerontology*, vol. 159, 2022.

C. GRANDI (a cura di), *I volti attuali del diritto penale europe*o, Pisa, 2021

CADOPPI A., CANESTRARI S., PAPA M.,MANNA A. (dir. da), *Cybercrime*, UTET Giuridica, 2019.

CARNALDO L., *L'istituzione del procuratore europeo e la tutela penale degli interessi finanziari dell'Unione europea*, Torino, Giappichelli, 2014.

CASADEI T., PIETROPAOLI S., *Diritto e Tecnologie informatiche*, CEDAM, 2021;

CAVALIERE A., *Associazione per delinquere*, in (MOCCIA S.)*Trattato di diritto penale. Parte speciale*, vol.V - *Delitti contro l'ordine pubblico*, Edizioni scientifiche italiane, 2007, pagg. 222-379.

CAVALIERE A.*, Tipicità ed offesa nei reati associativi*, in PATALANO V. (a cura di), *Nuove strategie per la lotta al crimine organizzato transazionale*,Giappichelli Editore, 2003.

CHELI E., *Libertà di associazione e poteri di polizia: profili storici*, in BARILE P. (a cura di),*La pubblica sicurezza,* Casa editrice Neri Pozza,1967, pag. 275 e ss.

CHOI K.,*Computer crime victimization and integrated theory: An empirical assessment*, in *International Journal of Cyber Criminology*,Vol.2, 2008, pagg. 308–333.

CHOO KIM-KWANG R., SMITH R. G., *Criminal Exploitation of Online Systems by Organised Crime Groups,* in *Asian Journal of Criminology*, vol. 3, n. 1, 2008,pagg. 37-60 (DOI: 10.1007/s11417-007-9035-y).

CHRISTEN M., GORDJIN B., LOI M., *The Ethics of Cybersecurity*, Springer International Publishing AG,2020 (DOI: https://doi.org/10.1007/978-3-030-29053-5/).

CIURCINA M., *Etica Hacker?,* in *DigitCult - Scientific Journal on Digital Cultures*, [S.l.], vol. 5, n. 1, 2020, pagg. 67-76 (DOI: https://doi.org/10.4399/97888255361647)

CLOUGH J., *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation,* in: *Monash University Law Review*, vol. 40 n. 3, 2014, pagg. 698-736; *Monash University Faculty of Law Legal Studies Research Paper*, n.6, 2015.

CLOUGH J., *The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World,* in *Criminal Law Forum*, vol.23, 2012,pagg.363–391 (DOI: https://doi.org/10.1007/s10609-012-9183-3/).

COHEN L. E., FELSON M., *Social change and crime rate trends: A routine activity approach*, in *American Sociological Review*, vol.44(4),1979, pag. 588 – 608

CONIGLIARO S. C., *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della nuova direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *Archivio Diritto Penale Contemporaneo*, 2013, pagg. 1-9 https://archiviodpc.dirittopenaleuomo.org/upload/1383078657CIVELLO%20CONIGLIARO%202013a.pdf

CONSULICH, *Reati contro l'ordine pubblico*, in ANTOLISEI F. (agg. a cura di GROSSO), *Manuale di diritto penale. Parte speciale*, vol. II, Giuffré, 1954.

CONSULICH, *Reati contro l'ordine pubblico*, in ANTOLISEI F. (agg. a cura di GROSSO),*Manuale di diritto penale. Parte speciale*, vol. II, Giuffré, 1968.

CONSULICH, *Reati contro l'ordine pubblico*, in ANTOLISEI F. (agg. a cura di Grosso), *Manuale di diritto penale. Parte speciale*, vol. II, Giuffré,2016, pagg. 113-123.

CORSO G., voce *Ordine Pubblico (dir. pubbl.)*, in *Enciclopedia del Diritto*, Volume XXX, Giuffrè, 1980.

COSIMI S., *Altro che Deep Web, il cyber crimine è di casa sui social network*, *La Repubblica.it*, 28/09/2016 (https://www.repubblica.it/tecnologia/sicurezza/2016/09/28/news/cybercrimine_altro_che_deep_web_sui_social_network_e_di_casa-148645562/).

COST B., *AI clones teen girl's voice in $1M kidnapping scam: "I've got your daughter", The New York Post.com*, 12/04/2023 (https://nypost.com/2023/04/12/ai-clones-teen-girls-voice-in-1m-kidnapping-scam/).

CUEVAS C. A., RENNISON C. M., *The Wiley Handbook on the Psychology of Violence*, Blackwell Pub, 2016.

DE FRANCESCO G. M., (voce) *Associazione per delinquere e associazione di tipo mafioso*, in *Digesto delle discipline penalistiche*, vol. I, UTET, 1987.

DE FRANCESCO G., *SocietasSceleris.Tecniche repressive delle associazioni criminali*, in *Rivista Italiana di diritto e procedura penale*, vol. I, 1992, pagg.55-148

DE MARSICO A., *Diritto penale - Parte generale*, Jovene, 1937.

DE ROSA V., *La formazione di regole giuridiche per il 'cyberspazio'*, in *Il diritto dell'informazione e dell'informatica*, vol.19, fasc.2 , 2003, pagg. 361-400.

DE VERO G., *Istigazione, libertà di espressione e tutela dell'ordine pubblico,* in *Archivio Penale,* vol. II,1976, pag. 3 e ss.

DE VERO G., *I reati associativi nell'odierno sistema penale,* in *Rivista Italiana di Diritto e Procedura Penale*, 1998, pag. 389 e ss.

DE VERO G., *Tutela dell'ordine pubblico e reati associativi*, in*Rivista Italiana di diritto e procedura penale*, 1993, pag. 107 e ss.

DE VERO G., *Tutela penale dell'ordine pubblico. Itinerari ed esiti di una verifica dogmatica e politico-criminale,* Giuffrè, 1988.

DE VIVO M. C., RICCI G.,*Diritto,Crimini e tecnologie*, in *Informatica e diritto*, XXXVIII Annata, vol. XXI, n.2, 2012, pagg. 25-112.

DELLA MORTE G., *Big data e protezione internazionale dei diritti umani*. *Regole e conflitti*, Editoriale scientifica, 2018.

DEN CATALDO NEUBURGER L. et al. *Anatomia del crimine in Italia : manuale di criminologia*. Giuffrè, 2013

DI CORINTO A., *Anonymous Italia contro il governo: le università nel mirino degli hacker*, *LaRepubblica.it*, 29/10/2018 (.https://www.repubblica.it/tecnologia/sicurezza/2018/10/29/news/anonymous_italia_contro_il_governo_le_universita_nel_mirino_degli_hacker-210320656/).

DI CORINTO A., *Anonymous: "Abbiamo violato la rete jihadista*", *LaRepubblica.it*, 08/02/2015(https://www.repubblica.it/tecnologia/2015/02/08/news/anonymous_abbiamo_violato_la_rete_jihadista-106820821/).

DI CORINTO A., *Che cos'è il Tor project e a cosa serve*, *La Repubblica.it*, 3/11/2017. (https://www.repubblica.it/tecnologia/sicurezza/2017/11/03/news/che_cos_e_tor_e_a_che_cosa_serve-180152431/).

DI CORINTO A., *Tutti i Segreti del Deep Web*, *La Repubblica.it*, 20/04/2014. (https://www.repubblica.it/tecnologia/2014/04/20/news/tutti_i_segreti_del_deep_web-84053410/).

DOLCINI E., *Appunti su <<criminalità organizzata>> e reati associativi,* in*Archivio Penale*, num. 2, Maggioli Editore, 1982,pp. 263-280.

DONINI M., *Integrazione Europea e Scienza Penale*, in *Rivista Trimestrale di Diritto Penale e dell'Economia*, vol. 3-4, 2020, pagg. 534-552.

DONNER C. M., MARCUM C. D., JENNIGS W. G., HIGGINS G. E., BANFIELD J.,*Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy*, in *Computers in Human Behaviour*, Vol.34, 2014,pagg. 165-172 (DOI: https://doi.org/10.1016/j.chb.2014.01.040/).

EUSEBI L.,*Anonimato, identità personale e diritto di cronaca nel mondo telematico. La sentenza della Corte di Cassazione n.5525/2012*, in *Ciberspazio e diritto*, vol.14, n.48, 2013, pagg. 183-209

FAGAN A. A., MAZEROLLE P., *Repeat Offending and Repeat Victimization: Assessing Similarities and Differences in Psychosocial Risk Factors* in *Crime &Delinquency*, Vol.*57*, Issue 5, 2011, pagg.732–755

FEDELI P., RICCI G., CORTUCCI C., *Lineamenti di Criminologia,cit.,* Edizioni Scientifiche Italiane, 2006, pag. 163 e ss

FEDELI P., RICCI G., CORTUCCI C., *Lineamenti di Criminologia,* Edizioni Scientifiche Italiane, 2006.

FIANDACA G., MUSCO E., *Diritto Penale - Parte Speciale*, vol. I, Zanichelli Editore, 1997.

FIANDACA G., MUSCO E., *Diritto Penale Parte Speciale*, Vol. I, Zanichelli Editore, 2021.

FIOCCA M. T., *Il darkside del cosmo digitale:"bersaglio- giovani". Le tutele*, in *Ciberspazio e diritto*, vol.20, n. 63, 2019, pagg. 475-494;

FIORE C., *Il reato impossibile*, Jovene, 1959.

FIORE C., voce *Ordine Pubblico (pen.),* in *Enciclopedia del Diritto*, Volume XXX, Giuffrè, 1980.

FOGGETTI N., *Il superamento del principio di territorialità. Quale diritto applicare ad Internet*, in *Ciberspazio e diritto*, Vol.5, n.3,2004, pagg. 231-241.

FORTI G., SEMINARA S., ZUCCALÁ G., *Commentario breve al codice penale*, CEDAM, 2017.

FOWLER T., *Cybersecurity*, in *Enterprise Risk Management. A Common Framework for the Entire Organization*, Green Philip E., Butterworth-Heinemann,2016, pagg. 91-108. (DOI: https://doi.org/10.1016/B978-0-12-800633-7.00007-9/).

FRANCESCHINI E.,*Anonymous e la guerra cibernetica in Ucraina. Domande e risposte per capire gli attacchi degli hacker, LaRepubblica.it*, 24/03/2022. https://www.repubblica.it/esteri/2022/03/24/news/anonymous_e_la_guerra_cibernetica_in_ucraina_domande_e_risposte_per_capire_gli_attacchi_degli_hacker-342704238/.

FRANCIONE G., *Hacker. I Robin Hood del Cyberspazio,* Lupetti, 2004.

FRIEDMAN J., Bouchard M., *Defintive Guide to Cyber Threat Intelligence*, Cyber Edge Press, 2015.

FROSINI T. E., *Il Costituzionalismo nella società tecnologica*, in *Diritto dell'Informazione e dell'Informatica*, volume 36, fascicolo 3, 2020, pag. 465-484.

GEORGE J. J., LEIDNER D. E., *From clicktivism to hacktivism: Understanding digital activism*, in *Information and Organization,* Volume 29, Issue 3, 2009. (DOI: https://doi.org/10.1016/j.infoandorg.2019.04.001./).

GILLEPSIE A. A., *Child Protection on the Internet Challenges for Criminal Law*, in *Child and Family Law Quarterly*, Volume 14, number 4,2002,pagg. 411-425.

GOTTFREDSON M. R., HIRSCHI, *A general theory of crime,* Stanford University Press, *1990*.

GÖTTKER, *The big five personality structure as a predictor for victimization in the context of cyber-crime*, University of Twente, Faculty of BMS: Behavioural, Management and Social Sciences,2021 (https://purl.utwente.nl/essays/87601).

GOUCHER, W., *Being a cybercrime victim,* in *Computer Fraud & Security*, Issue 10, 2010, pag.16-18, (DOI: https://doi.org/10.1016/S1361-3723(10)70134-2).

GRABOSKY P., *The Internet, Technology, and Organized Crime*, in *Asian Journal of Criminology,* 2007, Vol. 2, pag.145-161.(DOI: 10.1007/s11417-007-9034-z).

GRABOSKY P., *Virtual Criminality: Old wine in new bottles?,*in *Social & Legal Studies*, Volume 10, Issue 2,, 2001, pagg. 243-249 (DOI: https://doi.org/10.1177/a017405).

GRISPIGNI F., *Diritto Penale Italiano,* Vol.II, Giuffrè, 1947.

GROSSO C. F., *Le fattispecie associative: Problemi dommatici e di politica criminale,* in *Rivista Italiana di diritto e procedura penale*, vol. I, 1992, pagg.413-422

GUASTELLA G., *Il dominio geopolitico dello spazio cibernetico*, Edizioni Ex Libris, 2020.

GURUMURTHY A., MENON N., *Violence against Women via Cyberspace*, in *Economic and Political Weekly*, vol. 44, num. 40, 3/09/2009, pagg. 19-21.

HALL R. C.W., HALL R.C.W., *A profile of pedophilia: definition, characteristics of offenders, recidivism, treatment outcomes, and forensic issues*, in *Mayo Clinic proceedings,* Volume 82, Issue 4, 2007, pagg.457-471. (DOI:https://doi.org/10.4065/82.4.457).

HERZOG-EVANS M., *Transnational Criminology Manual*, Vol.1, Wolf Legal Publishers, 2010.

HOLT T. J., BOSSLER A., MAY D., *Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance*, in *American Journal of Criminal Justice,* 2012, Volume .37, Issue 3, pagg. 378-395 (DOI:https://doi.org/10.1007/s12103-011-9117-3/)

HOLT T. J., KILGER M., *Know your enemy: The social dynamics of hacking*,*Honeynet Project.org*, 2012, pagg.1-7 (DOI: https://www.honeynet.org/download/paper-know-your-enemy-the-social-dynamics-of-hacking/).

HOLT T. J., SCHELL B.H. *Corporate hacking and technology-driven crime: Social dynamics and implications*, NY: Information Science Reference,2011, New York.

HOLTT. J., LAMPKE E.,*Exploring stolen data markets online: products and market forces*, in *Criminal Justice Studies: A Critical Journal of Crime, Law, and Society*, vol.23, Is.1,2010, pagg.33–50.(DOI: https://doi.org/10.1080/14786011003634415).

IACOVIELLO F. M., *Il concorso eventuale nel delitto di partecipazione ad associazione per delinquere*, in *Cassazione Penale*, 1995, pagg. 858 e ss.

IACOVIELLO F. M., *Ordine Pubblico e associazione per delinquere,* in *La Giustizia Penale*, parte II, 1990, pp.38-64.

INGROIA A., *L'associazione di tipo mafioso,* Giuffrè, 1993.

INSOLERA G., *L'associazione per delinquere,* CEDAM, 1982.

INSOLERA G.*, Sulle diverse forme di criminalità organizzata*, in Angeli F.,*Beni e tecniche della tutela privata*,1986.

ITALIA MINISTERO DI GRAZIA E GIUSTIZIA, FONDAZIONE CENTRO INTERNAZIONALE SU DIRITTO SOCIETÁ ED ECONOMIA, *I reati associativi*, Giuffrè, 1998.

JARDINE E., *The Dark Web Dilemma: Tor, Anonymity and Online Policing,* in *Global Commission on Internet Governance Paper Series,* num.21,2017, pagg.37-50.(DOI: http://dx.doi.org/10.2139/ssrn.2667711).

JAVAHERI D., GORGIN S., Lee J., MASDARI M., *Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspective*, in *Information Sciences*, vol. 626, 2023,pagg. 315-338 (DOI: https://doi.org/10.1016/j.ins.2023.01.067).

JOHN O. P., ROBINS R. W., *Handbook of personality: Theory and research*, Guilford Press, 1999.

KRANENBARG M. W.,LEUKFELDT R., *Cybercrime in context: The human factor in victimization, offending and policing*, Springer International Publishing AG, 2021.

KRANENBARG M. W., VAN GELDER J., BARENDS A. J., DE VRIES R. E., *Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets,*in *Computers in Human Behaviour,* Vol.140*,* 2023(DOI: https://doi.org/10.1016/j.chb.2022.107576/).

KRANENBARG M. W., RUITER S., VAN GELDER J., *Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap*, in *Deviant Behavior*, vol.40, Issue 1, 2019,pag.40-55 (DOI:10.1080/01639625.2017.1411030/).

KRANENBARG M. W., RUITER S., VAN GELDER J.,BERNASCO W., *Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe,* in *International Conference On Cyber Situational Awareness, Data Analytics And Assessment,* 2017, Londra, pagg.1-8. (DOI: 10.1109/CyberSA.2017.8073391/.)

KRANENBARG M. W., RUITER S., VAN GELDER J., BERNASCO W., *Cyber-Offending and Traditional Offending over the Life-Course: an Empirical Comparison,* in *Journal of Developmental and Life-Course Criminology*, Vol. 4, Issue 3, 2018, pagg. 343-364. (DOI: 10.1007/s40865-018-0087-8/).

KSHETRIN., *Diffusion and Effects of Cyber-Crime in Developing Economies*, in *Third World Quarterly*, Vol. 31, num.7, 2010, pagg. 1057-1079 (https://www.jstor.org/stable/27896600/).

LAMBERTI C., *Gli strumenti di contrasto al terrorismo e al cyber-terrorismo nel contesto europeo,* in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. VIII, num. 2, 2014,pagg. 138-161.

LANDERS C., *Serious business: Anonymous takes on Scientology (and doesn't afraid of anything)*, *Baltimore City Paper,* num. 4, 2/04/2008.

LATTANZI G., LUPO E., *Codice penale. Rassegna di giurisprudenza e di dottrina*, vol. IX, 2010,Giuffrè.

LAURITSEN J. L., SAMPSON R. J., LAUB J. H., *The link between offending and victimization among adolescents*, *cit.,* in *Criminology*, volume 29, Issue 2, 1991, pagg. 264-292 (DOI: https://doi.org/10.1111/j.1745-9125.1991.tb01067.x).

LAVACCA G., ARTINI C. M., PELLEGRINO M., *Internet never forgets(?). Diritto all'oblio e diritto alla cancellazione, quali gli usi e quali i limiti*, in *Ciberspazio e Diritto*, vol 20, n. 63, 2019, pagg. 437-461.

LAVAGNA C., *Il concetto di ordine pubblico alla luce delle norme costituzionali*, in *Democrazia e Diritto*, n.3-4, 1967, pp.359-381

LAVOGRNA A., *Guardando oltre la criminalità informatica: l'importanza dell'approccio criminologico del "danno sociale" per osservare il ciberspazio con sguardo critico*, in *Ciberspazio e Diritto*, vol. 22, num. 67, 2022, pagg.41-58.

LAVORGNA A., *Cyber-organised crime. A case of moral panic?,*in *Trends in Organized Crime* , vol. 22, Issue 4, 2019, pagg.357–374 (DOI: https://doi.org/10.1007/s12117-018-9342-y).

LAVORGNA A., *Organised crime goes online: realities and challenges*, in *Journal of Money Laundering Control*, Vol. 18, N. 2,2015,pagg. 153-168. (DOI: https://doi.org/10.1108/JMLC-10-2014-0035).

LAVORGNA A., HOLT T. J., *Researching Cybercrimes. Methodologies, Ethics, and Critical Approaches,* Palgrave Macmillan Cham, 2021 (DOI: https://doi.org/10.1007/978-3-030-74837-1/).

LEE K., ASHTON M. C., *Psychometric properties of the HEXACO personality inventory, in Multivariate Behavioral Research,* Volume 39,Issue 2,2004,pagg. 329-358(DOI: https://doi.org/10.1207/s15327906mbr3902_8).

LEO G., *L'associazione a delinquere finalizzata al traffico di stupefacenti (Art. 74 D.P.R. n. 309/90)*, in CADOPPI, CANESTRARI, MANNA, PAPA, *Trattato di Diritto Penale*, *Parte Speciale*, Vol. IV, UTET Giuridica, 2010, pag.702 ss.

LESSIG L., *Code and Other Laws of Chyberspace*, Basic Books,2006.

LEUKFELDT E. R., HoltT. J., *Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals,* in *Computers in Human Behaviour*, Vol.126, 2022. (DOI:https://doi.org/10.1016/j.chb.2021.106979/)

LEUKFELDT E. R., Kleemans E. R., StolW., *Cybercriminal networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks*, in *British Journal of Criminology*, Volume 57, Issue 3, pagg. 704-722 (DOI: https://doi.org/10.1093/bjc/azw009).

LEUKFELDT R., *Research Agenda. The Human Factor in Cybercrime and in Cybersecurity*, Eleven International Publishing 2017.

LI V., *Cacciatori di bug. Guida per imparare a trovare e riportare vulnerabilità web*, Apogeo, 2023.

LOEVINGER L., *Jurimetrics:The Next Step Forward*, in *Minnesota Law Review*, vol. 33, 1949, pag.455 e ss.

LUGATO M., *Il << discorso d'odio>>. Le coordinate giuridiche del ragionamento internazionalistico*, in *Rivista di Dirito Internazionale*, 2022, fasc.4, pag. 959 e ss. .

MAGGIPINTO A.,*Reati nella Rete, tutti i nodi da sciogliere. Se il cybercrime mette in crisi il Codice*, in *Diritto& Giustizia,* vol.6,2006, pagg. 61-63.

MAIETTA A., *In tema di I.A.D., internet addiction disorder,* in *Diritto Di Internet*, fascicolo 2, 2007, pagg.199-201.

MANZINI V., *Trattato di diritto penale italiano,* (a cura di) NUVOLONE, PISAPIA, UTET, 1981.

MANZINI V.,PISAPIA G. D.,*Trattato di Diritto penale*, UTET, 1983.

MARCIANO G., *Associazione per delinquere e concorso criminoso*, in I.d., *Questioni di diritto*, (con note di) Altavilla E., Morano, 1926.

MARCIANO G.*, Associazione per delinquere e concorso criminoso,* in *Questioni di diritto* (con note di Altavilla E.), Editore Morano, Napoli, 1926.

MARINI A., voce (*Delitti contro) l'Ordine Pubblico,* in *Novissimo Digesto Italiano*, (diretto da) Azara ed Eula, vol. V, UTET, 1984.

MAROTTA G., *Tecnologie dell'informazione e nuovi processi di vittimizzazione,* in *RivistaQuadrimestrale di Criminologia, Vittimologia e Sicurezza,*vol. VI, n.2,2012, pagg.93-106.

MAROZ N.*, Regionalization of International cooperation in the fight against Cybercrime*, in *Law Review* (Romania), vol.X, Issue 2, 2019,pagg. 218-227.

MARTINES T.,*Diritto Costituzionale*, Giuffrè, 1992.

MATTARELLA A., *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Diritto penale e processo*, vol.6, 2022,pagg. 809-829.

MATTARELLA A., *La futura Convenzione ONU sul Cybercrime e il contrasto a nuove forme di criminalità informatica*, in *Sistema Penale*, vol.3,2022, pag. 41-75 (DOI: https://www.sistemapenale.it/it/fascicoli/fascicolo-mensile-2022-3/).

MATULESSY A., HUMAIRA N. H., *Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits*, in *Psychology and Behavioral Sciences*., Vol. 5, n. 6,2016,pagg. 137-142 (DOI: 10.11648/j.pbs.20160506.12).

MAURUSHAT A., *Australia's Accession to the 'Cybercrime Convention': Is the 'Convention' Still relevant in combating Cybercrime in the era of botnets and obfuscation crime tools*?, in *University of New South Wales Law Journal*, Vol. 33, No. 2, 2010, pagg. 431-473.

MAZZUCA T., *L'origine dei maxiprocessi e le vie del loro superamento*, in *Anatomia del maxiprocesso (Atti del Convegno),* in *Difesa penale*, n. 16-17,1987, p. 23.

MC CUSKER R., *Transnational organised cybercrime: distinguishing threat from reality*, in *Crime Law and Social Change*, 6, pagg. 257-273,2006(DOI: 10.1007/s10611-007-9059-3).

MC GUIRE M., *Organised crime in the digital age*, cit. , John Grieve Centre for Policing and Security and BAE Systems Detica,2012(http://www.baesystemsdetica.com/uploads/resources/ORGANISED_CRIME_IN_THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf).

MELCHIONDA A., PICOTTI L., FORNASARI G., VIGANÓ F.,*I reati associativi: paradigmi concettuali e materiale probatorio. Un contributo all'analisi e critica del diritto vivente*, CEDAM, 2005.

MELE P.,*La guerra di Anonymous all'Isis. Intervista ad Antonino Caffo, Archivio di RaiNews.it*, 24/12/2015(https://www.rainews.it/archivio-rainews/articoli/guerra-di-Anonymous-Isis-Intervista-Antonino-Caffo-e41997f0-26f2-4638-b4f0-60e65337686e.html?refresh_ce).

MELUCCI A., *Challenging Codes: Collective Action in the Information Age,* Cambridge University Press, 1996.

MENN J., *They're watching. And they can bring you down,FinancialTimes.com*, 23/10/2011 (DOI: https://www.ft.com/content/3645ac3c-e32b-11e0-bb55-00144feabdc0).

MINISTERO DELLA GIUSTIZIA E DEGLI AFFARI DI CULTO, *Relazione ministeriale sul Progetto del codice penale* in *Lavori preparatori del codice penale e del codice di procedurapenale,* parte II,Tipografia delle Mantellate, Roma, 1929.

MONTHEITH S., BAUER M., ALDA M., GEDDES J., WHYBROW P. C., GLENN T., *Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry*, in *Current Psychiatry Rep*ort, Volume 23, Issue 4, 2021,pagg. 18-27. (DOI: 10.1007/s11920-021-01228-w).

MORIZOT J., KAZEMIAN L., *The development of criminal and antisocial behavior.Theory, Research and Practical Applications,* Springer, 2015 (DOI: https://doi.org/10.1007/978-3-319-08720-7/).

MOSCA G., *Anonymous Italia annuncia nuovi attacchi*, *Wired.It*, 29/10/2018 (DOI: https://www.wired.it/attualita/tech/2018/10/29/anonymous-italia-2018/).

MOUSTAFA A., *Cybersecurity and Cognitive Science*, Academic Press, 2022(DOI:https://doi.org/10.1016/B978-0-323-90570-1.00003-6).

MUSCATIELLO V. B., *Il concorso esterno nelle fattispecie associative,* CEDAM, 1995.

MUSOTTO R., Wall D. S., *More Amazon than Mafia: analysing a DDoS stresserservice as organised cybercrime*, in *Trends in Organized Crime*, Volume 25, Issue 2, 2022, pagg. 171-193. (DOI: https://doi.org/10.1007/s12117-020-09397-5/).

NEPPI MODONA G., *Criminalità organizzata e reati associativi*, in *Beni e tecniche della tutela penale,* a cura di Crs - Sezione politica e istituzioni in Europa, Franco Angeli Libri, 1987.

NEPPI MODONA G., *Il processo cumulativo nel nuovo codice di procedura penale*, in *Cassazione penale*, 1988

NICOLÓ G., POMPILI E., *Manuale Diagnostico e Statistico dei disturbi mentali*, Raffaello Cortina Editore, 2014.

NIVEAU G., *Cyber-pedocriminality: Characteristics of a sample of internet child pornography offenders*, in *Child Abuse & Neglection*, vol. 34, Issue.8, 2010, pagg.570-575 (DOI: 10.1016/j.chiabu.2010.01.01).

NUVOLONE P., *Il sistema del diritto penale*, CEDAM, 1975.

NUVOLONE P*., Le leggi penali e la Costituzione*, Giuffrè, 1953.

OLSON P.,*Noi Siamo Anonymous*, Edizioni Piemme, 2013.

ORTALDA A., LEUCCI S., *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Rivista italiana di informatica e diritto*, fasc.4, 2022,pagg.145-155.

PACE A., *Il concetto di ordine pubblico nella Costituzione Italiana,* in *Archivio Giuridico <<Filippo Serafini>>,* vol. XXIV, 1963.

PALAZZO F. C., *Associazioni illecite ed illeciti delle associazioni,* in *Rivista Italiana di Diritto e procedura penale,* 1976, pag. 418 e ss.

PALAZZO F. C., *Corso di diritto penale. Parte generale*, Giappichelli Editore, 2013.

PANATTONI B., *Iriflessi penali del perdurare nel tempo dei contenuti illeciti nel Cyberspace*, in *Sistema Penale*, vol.5, 2020,pagg. 303-324.

PAOLILLO J. C., *Language variation on Internet Relay Chat: A social network approach*, in *Journal of Sociolinguistics*, Volume 5 , Issue 2, 2001, pagg.183-210 (DOI: https://doi.org/10.1111/1467-9481.00147/).

PAPADIMITRIOU F., *A nexus of Cyber-Geography and Cyber-Psychology: Topos/''Notopia" and identity in hacking,* in*Computers in Human Behavior*, vol. 25, 2009, pag. 1331–1334. (DOI:https://doi.org/10.1016/j.chiabu.2010.01.011/).

PARODI C., CALICE A., *Responsabilità penali ed Internet. Le ipotesi di responsabilità penale nell'uso dell'informatica e della telematica*, Il Sole 24 Ore, collana Diritto, 2001.

PARODI C., SELLAROLI V., *Diritto Penale dell'Informatica. Reati della rete e sulla rete,* Giuffrè, 2009.

PASCUZZI G., *Il diritto dell'era digitale*, Il Mulino, 2020.

PATALANO V., *L'associazione per delinquere*, Jovene, 1971.

PAULHUS D., WILLIAMS K. M., *Thedark triad of personality: Narcissism, Machiavellianism, and psychopathy*, in *Journal of Research in Personality*, vol. 36, Issue 6, 2004,pagg. 556–563. (DOI: https://doi.org/10.1016/S0092-6566(02)00505-6/)

PAWLICA A., CHORÁS M., PAWLICKI M., *The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good*, in Personal and Ubiquitous Computing, vol.25, Issue 5,2021,pagg. 843–852. (DOI: https://doi.org/10.1007/s00779-021-01568-7).

PEZZELLA V., La diffamazione, UTET Giuridica, pagg. 1046 e ss. ;

PICA G., (voce) *Internet*, in Digesto delle discipline penalistiche, UTET, 2004.

PICOTTI L., *Il diritto penale dell'informatica nell'epoca di Internet,* CEDAM, 2005.

PICOTTI L., *Intercettazioni "illegali" tra nuove tecnologie e vecchi strumenti penali*, in *Diritto dell' Internet*, vol.2, 2007, pagg. 113-122.

PICOTTI L., *La nozione di <<criminalità informatica>> e la sua rilevanza per le competenze penali europee*, in *Rivista Trimestrale del Diritto Penale ed econom*ia, vol.4, 2011, pagg.827-864.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Diritto Penale e Processo*, n.6,2008, pagg. 700-716.

PONTI C., *Il diritto internazionale e la criminalità organizzata, inRivista di Studi e ricerche sulla criminalità organizzata,* vol.1,2015, pagg. 23-36.

PORRO G., *Che fine hanno fatto gli hacker per una giusta causa*?,*Wired.it*, 06/06/2019, (DOI: https://www.wired.it/internet/web/2019/06/06/hacker-attacco-anonymous/).

PORRO G., *Gli hacker di Anonymous pubblicano i dati di oltre 30mila avvocati (Raggi compresa),Wired.it*,07/05/2019, (DOI: https://www.wired.it/internet/web/2019/05/07/avvocati-italia-luzsecita/).

POWELL A., FLYNN A., SUGIURA L., *The Palgrave Handbook of Gendered Violence and Technology;* Palgrave MacMillian Cham, 2021.

PULITANÓ D., *Il favoreggiamento personale tra diritto e processo penale*, Giuffrè, 1984.

RADIANTI J., *A Study of a Social Behavior inside the Online Black Markets*., in AA.VV., *2010 Fourth International Conference on Emerging Security Information, Systems and Technologies*, IEEE, pagg.189-194. (DOI: DOI: 10.1109/SECURWARE17361.2010).

RAJAWAT A. S., BEDI P.,GOYAL S. B., KAUTISH S.,XIHUA Z., ALJUAID H., MOHAMED A. W., *Dark Web Data Classification Using Neural NetworK Computational intelligence and neuroscience*, 2022, 8393318. (DOI: https://doi.org/10.1155/2022/8393318).

RAMPIONI R., *Nuovi profili del reato continuato*, in *Rivista Italiana di Diritto e Procedura Penale*, 1978.

REEP VAN-DER-BERGH C., JUNGER M., *Victims of cybercrime in Europe: a report of victim surveys*, in *Crime Science,* Volume 7, 2018,pagg. 1-15.

RIONDATO S., *Competenza penale della Comunità europea. Problemi di attribuzione attraverso la giurisprudenza.* CEDAM, 1996.

RIONDATO S., FORNASARI G., *Reati contro l'ordine pubblico*, II ed., Giappichelli Editore, 2017.

RUGGIERO V., *Crimine organizzato e transnazionale in Europa*, in *Studi sulla questione criminale*, Vol. 2-3, 2015,pagg. 183-201.

SALERNO N., *Concorso delittuoso e associazione a delinquere,*in *Scuola positiva*, vol. I, 1930.

SANTORO A., *Manuale di Diritto Penale,* Vol. I, UTET, 1958.

SCHICKS J., VAN DE WEIJER S., LEUKFELDT R., *High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals,* in *Computers in Human Behaviour*, vol.126, 2022. (DOI: https://doi.org/10.1016/j.chb.2021.106985/).

SCHRECK C. J., et al., *Self-Control, Victimization, and Their Influence on Risky Lifestyles: A Longitudinal Analysis Using Panel Data,*in *Journal of Quantitative Criminology*, vol. 22, n. 4, 2006, pagg. 319–340, https://doi.org/10.1007/s10940-006-9014-y/

SCIRPA A., *Cybercrime e criminal profiling: i nuovi approcci delle tecniche investigative nell'era tecnologica*, in Ciberspazio e Diritto, vol. 20, num. 62, 2019, pagg. 297- 310.

SCORZA G., *In difesa dell'anonimato online. I leoni da tastiera non si battono eliminandolo*, in *Huffington Post*, 11/12/2022.

SCUDERI R., *Un caso di hacking: luoghi reali e luoghi virtuali tra diritto e informatica*, in *Ciberspazio e diritto*, vol. 7, num. 3,2006, pagg. 377-424.

SEEBRUCK R., *A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model,*in *Digital Investigation,* vol. 14, 2015, pagg. 36-45. (DOI: https://doi.org/10.1016/j.diin.2015.07.002.)

SEMINARA S., *Locus commissi delicti, giurisdizione e competenza nel cyberspazio*, relazione al Convegno "Presi nella rete - Analisi e contrasto della criminalità informatica", Pavia, 23 novembre 2012, consultato in data 04/06/2023(Https://www.flamminiiminutochiocci.it/public/pubblicazioni/Giurisdizione_italiana_per_diffamazione_internet_dall_es)

SEMINARA S., voce *Internet,* in *Enciclopedia del diritto*. *Annali*, vol.VII, Giuffrè, 2014.

SHINDER D. L., Cross M., *Scene of the Cybercrime,*Syngress ed., 2008 (DOI: https://doi.org/10.1016/B978-1-59749-276-8.00003-0/).

SICURELLA R. et al., *L' evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona ,* Pubblicazioni del Centro di Diritto Penale Europeo (Catania), 2011

SILIC M., LOWRY P. B., *Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes*, in *Information Systems Frontiers*, vol.23, Issue. 2, 2019,pagg. 339-341 (DOI: https://doi.org/10.1007/s10796-019-09949-3).

SINHA S., *Bug Bounty Hunting for Web Security: Find and Exploit Vulnerabilities in Web sites and Applications*, APress, 2019.

SLEIMAN M. B., GERDEMANN S., *Covid-19: a catalyst for cybercrime?*, in *International Cybersecurity Law Review* , vol. 2, Issue 1, 2021, pagg. 37–45 (DOI: 10.1365/s43439-021-00024-9).

SMITH R.G., CHEUNG R., YIU-CHUNG LAU L., *Cybercrime Risks and Responses*, Palgrave Macmillan, 2015(DOI: (https://doi.org/10.1057/9781137474162_14/).

SPAGNOLETTI P., CECI F., BYGSTAD B., *Online Black-Markets: An Investigation of a Digital Infrastructure in the Dark*, in *Information Systems Frontiers*, vol. 24, Is. 6,2022,pagg. 1811-1826. (DOI: https://doi.org/10.1007/s10796-021-10187-9).

SPAGNOLO G., *Criminalità organizzata e reati associativi: problemi e prospettive,* in *Rivista italiana di Diritto e Procedura Penale*, fascicolo 4, 1998,pagg. 1161-1168.

SPAGNOLO G*., Dai reati meramente associativi ai reati a struttura mista*, inCrs - Sezione politica e istituzioni in Europa, *Beni e tecniche della tutela penale,* Franco Angeli Libri, 1987, pag. 156 e ss.

SPAGNOLO G., *L' associazione di tipo mafioso,* CEDAM, 1993.

STAMBAUGH H., *Electronic crime needs assessment for state and local law enforcement,* US Department of Justice, Office of Justice Programs, National Institute of Justice,2001.

STEINMETZ K. F., *CRAFT(Y)NESS: An Ethnographic Study of Hacking*, in *The British Journal of Criminology,* vol.55, Issue 1,2015, pagg. 125–145 (DOI:http://www.jstor.org/stable/43819263/).

STRANO M., *Manuale di criminologia clinica*, SEE Editrice Firenze,2003.

SULER J., *The online dishinibition effect*, in *Cyberpsycology &Behaiviour,* vol.7, Issue 3, 2004, pagg. 321-326.

TADDEI E.G., *L'informatica giuridica: disciplina o ricerca?,*in *Ciberspazio e diritto*, vol.7, num. 2, 2006,pagg. 244-251.

TADDEI E. G., PERUGINELLI G., *Dall'informatica giuridica al diritto dell'internet*, in *Diritto di Internet*, fascicolo 6, 2006, pagg. 113-116.

TEHRANI A. G.K., PONTELL H., *Phishing Evolves: Analyzing the Enduring Cybercrime*, in *Victims & Offenders*, vol.16, n.3,2021, pagg.316–342 (DOI:10.1080/15564886.2020.1829224).

TEICHMANN F.M.J., SERGI B.S., WITTMANN C., *The compliance implications of a cyberattack: a distributed denial of service (DDoS) attack explored*, in *International Cybersecurity Law Review*, 2/06/2023, pagg.1-7. (DOI: https://doi.org/10.1365/s43439-023-00090-1).

TELEFONO ARCOBALENO ONLUS- Centro studi e ricerche sull'abuso d'infanzia, *International Observatory Against Child Abuse and Sexual Exploitation,* Short Report- April 2011; pagg. 1-6.(https://www.dmi.unict.it/~battiato/CF1011/ShortReport-aprile2011.pdf).

TENBARGE K., *Found through Google, bought with Visa and Mastercard: Inside the deepfake porn economy*, *Nbc News.com*, 26/03/2023. (https://www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071)

TONA G., *I reati associativi e di contiguità (artt. 416-8)*, in CADOPPI A., CANESTRARI

S.,MANNA A., PAPA M., *Trattato di Diritto Penale-Parte Speciale, Vol.III*, UTET Giuridica, 2008, pagg. 1063-1155.

TONELLOTTO M., *Criminalità e cyberspazio, alcune riflessioni in materia di cyber criminalità,* in *Rivista Quadrimestrale di Criminologia, Vittimologia e Sicurezza*, vol. XVI, 2022,pagg. 6-21.

TORRENTE A., SCHELSINGER P., *Manuale di Diritto Privato*, Giuffrè, 1995.

TOSI E., *Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè, 2019.

TRABUCCHI A., *Manuale di Diritto Civile*, 47esima edizione, CEDAM, 2015.

TRAVAINI G., CARUSO P., MERZAGORA I., *Crime in Italy at the time of the pandemic,* in *Acta bio-medica: AteneiParmensis*, vol. 91, Issue 2,2020, pagg.199-203. (DOI:10.23750/abm.v91i2.9596).

TURANOVIC J., PRATT T., "*Can't Stop, Won't Stop": Self-Control, Risky Lifestyles, and Repeat Victimization,* in *Journal of quantitative criminology,* Vol.30, Issue 1,2014, p.29-56 (DOI:10.1007/s10940-012-9188-4).

UN OFFICE ON DRUGS AND CRIME (UNODC), *Computer related-crime,* The Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 18-25 April 2005, Bangkok, Thailand (http://unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf).

UNICEF, *The State of the World's Children in a digital world,*2017, pagg. 76-90 (https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf).

UNITED NATIONS OFFICE AT VIENNA- Centre for Social Development and Social Affairs, *International Review of Criminal Policy, Nos. 43 and 44,*United Nations, 1994.

VAN DE WEIJER S., LEUKFELDT R., *Big Five Personality Traits of Cybercrime Victims*, in *Cyberpsychology, Behaviour, and Social Networking*, Vol.20, Issue 7,2017,pagg. 407-412. (DOI: 10.1089/cyber.2017.0028/).

VAN DER HOF S., KOOPS B-J., *Adolescents and Cybercrime: Navigating between Freedom and Control*, in *Policy & Internet*, Vol. 3, Issue 2, Article 4, 2011(DOI: 10.2202/1944-2866.1121).

VAN WILSEM J., '*Bought it, but never got it'. Assessing risk factors for online consumer fraud victimization. cit.,* in *European Sociological Review*, vol. 29, Issue 2, 2013,pagg. 168–178 (DOI: https://doi.org/10.1093/esr/jcr053/).

VERMA P., *Their voices are their livelihood. Now AI could take it away, The Washington Post.com*, 24/04/2023. (https://www.washingtonpost.com/technology/interactive/2023/ai-voice-generators/).

VIANO E. C. , *Cybercrime, Organized Crime, and Societal Responses International Approaches*; International Publishing AG, 2017(DOI: https://doi.org/10.1007/978-3-319-44501-4).

VILASI F., *La strategia dell'Unione Europea per la lotta alla criminalità organizzata:la centralità dell'informazione e le prospettive di riforma futura,*in *Rivista di Studi e ricerche sulla criminalità organizzata,* Vol.7, 2021.

VIRTANEN S. M., *Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities,* in *Psychiatry, Psychology and Law*, volume 24, Issue 3, 2017, pag.323-338 (DOI: 10.1080/13218719.2017.1315785).

VOLPICELLI E., D'ERRICO G., *Anonymous, nuovi supereroi contro le forze del male?*, *Il FattoQuotidiano.it*, 11/01/2016(https://www.ilfattoquotidiano.it/2016/01/11/anonymous-nuovi-supereroi-contro-le-forze-del-male/2363875/).

WALKER S., TENNANT I., *Control, alt or delete? The UN Cyber crime debate enters a new phase, Global Initiative against transnational organized crime* , 2021(https://globalinitiative.net/wp-content/uploads/2021/12/UN-Cybercrime-PB-22Dec-web.pdf)

WIENER N., *Cybernetics: Or Control and Communication in the Animal and the Machine*, The M.I.T Press, 1948.

WIGGINS L. M., *Corporate Computer Crime: Collaborative Power in Numbers,*in *Federal Probation*, Vol. 66, Issue 3, 2002,pagg. 19-29.

YOUNG R., ZHANG L., PRYBUTOK V., *Hacking into the Minds of Hackers*, in *Information Systems Management,*2007, Volume 24, number 4, pagg. 281-287(DOI: https://doi.org/10.1080/10580530701585823/).

ZAAMI S., *New Psychoactive Substances and evolving criminal dynamics against the backdrop of the fourth industrial devolution,* in *Acta Biomed*, Vol. 93, N. 2.,2022, (DOI: 10.23750/abm.v93i2.13008)

ZICCARDI G.*, I virus informatici: aspetti tecnici e giuridici*, in *Ciberspazio e Diritto*, Volume 2, numeri 3-4,2001, pagg. 347-363.

ZICCARDI G., *L' odio online : violenza verbale e ossessioni in rete*, R. Cortina, 2016.

ZUCCALÁ G., *Personalità dello Stato, ordine pubblico e tutela di libertà di pensiero,* in *Rivista Italiana di Diritto e Procedura penale,* 1966.

Note a sentenza

APREA F., *Sugli elementi costitutivi dell'associazione a delinquere* (nota alla sentenza Cassazione penale, Sezione III n. 41528 del 24/11/2010) in *Giurisprudenza Italiana,* fascicolo 7/2011, pagg. 1624-1627.

BURZI E.*, Nota sui requisitiper la sussistenza del reato di associazione per delinquere (*nota alla sentenza Cassazione Penale, Sez. I n. 39757 del 28/9/2005), in *Giurisprudenza Italiana*, fascicolo 7/2006, pagg. 1483-1485

CATULLO F. G., *Ai confini della responsabilità penale: che colpa attribuire a Google*, (nota alla sentenza del Tribunale Milano sez. IV, n.1972 del 12/04/2010) in Giurisprudenza Di Merito, 2011 fasc.1, pagg. 0159B e ss.;

CORVI A., *Alla ricerca del "fatto" penalmente rilevante nei delitti associativi* (nota alla sentenza Cassazione penale, sez. V n. 695 del 03/12/2013), in *Rivista Italiana di Diritto e Procedura Penale*, fascicolo 1/2015, pagg. 375-386

CORVI A., *Requisiti e limiti della "partecipazione" nel reato di associazione a delinquere* (nota alla sentenza Cassazione Penale, sez. II, numero 49691 del 28/12/2004) in *Diritto Penale e Processo,* n. 5/2005, pagg. 600-607.

DEL CORSO S., *I nebulosi confini tra associazione per delinquere e concorso di persone nel reato continuato*, (nota alle sentenze: Cassazione Penale Sez. I del 30/04/1979, Reale, in *Giustizia Penale*, 1979, vol. II; Cassazione Penale Sez. I del 28/03/1979, Pizzo, in *Rivista Penale*, 1980, pag. 83),in *Cassazione Penale,* 1985, vol. IV., pagg. 621-627.

EUSEBI L., *Anonimato, identità personale e diritto di cronaca nel mondo telematico. La sentenza della Corte di Cassazione n. 5525/2012*, in *Ciberspazio e diritto*, vol. 14 n.48 (2-2013), pagg. 183-209;

FLOR R., *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, (nota alla sentenza Cassazione Penale, Sezioni Unite, n.17325 del 26/03/2015), in *Diritto Penale e Processo*, 2015, numero 10, pagg.1296-1310.

FRANCESCHELLI V., *Sul controllo preventivo del contenuto dei video immessi in rete e i provider. A proposito del caso Google/Vivi Down.* (nota alla sentenza del Tribunale Milano sez. IV, n.1972 del 12/04/2010), in *Rivista di Diritto Industriale,* fasc.4-5, 2010, pagg. 347 e ss.;

MAZZINI G., *Prevalenza del diritto comunitario e non obbligatorietà della legge penale: un rapporto interessante, ma non sostenibile,* (nota alla sentenza Trib. Milano del 1/3/2000, in *Rivista italiana di diritto e procedura penale,* 2002, fasc. 1, pagg. 361-368), in *Rivista italiana di diritto e procedura penale,* 2002, fasc. 1, pagg. 368-380.

MIGLIO M., *Brevi appunti in merito alla necessaria distinzione tra associazione a delinquere e concorso di persone nel reato continuato* (nota alla sentenza Corte di Appello di Roma, Sez. III, n. 2984 del 31/03/ 2016), in Giurisprudenza Penale Web, fascicolo 12/2016.

MISAGGI M. C., *Associazione per delinquere e concorso di persone nel reato continuato: il confine è davvero sottile?,*nota alla sentenza a Cassazione Penale, Sez. III, numero 11570 del 30 gennaio 2020, in *Rivista Scientifica Diritto Penale E Uomo,* fascicolo 9/2020, pagg.84-96.

STRAMAGLIA M., *L'associazione per delinquere nell'era della realtà virtuale*, (nota alla sentenza Trib. Siracusa, n. 229 del 19/07/2012), in *Giurisprudenza di Merito*, 2013, fasc.11, pag. 2434-2442.

Giurisprudenza

Cassazione penale del 15/07/1949, in *Giustizia Penale*, 1949, vol. II, pag.895.

Cassazione penale del 31/3/1952, in *Giustizia Penale*, 1952, vol.II, pag. 814.

Cassazione penale, sez. III, del 10/05/1961, in *Cassazione Penale*, 1961, vol.II, pag. 811;

Cassazione penale sez. I del 26/10/1977, in *Cassazione Penale*, 1979, pag.306.

Cassazione penale, sez. I del 14/11/1980, in *Giustizia Penale*, 1981.

Cassazione penale, sez. I del 13/01/1983, in *Giurisprudenza Italiana*,1983, Vol.II, pag.353.

Cassazione penale, sez. II del 08/07/1983,in *Cassazione Penale*, 1985, pag. 866.

Cassazione penale, sez. I del 16/11/1984, in *Giustizia Penale*, 1985, Vol. II, pag.616.

Cassazione penale, sez. I del 23 aprile 1985, in *Foro Italiano*, 1986, Vol. II, pag. 595.

Cassazione penale, sez. I del 27/01/1986 in *Cassazione Penale*. 1987, pag. 1719.

Cassazione penale, sez. II del 15/04/1986, in *Rivista Penale*, 1986, pag.955.

Cassazione penale, sez. VI n. 14701 del 15/10/1986, in C.E.D. Cassazione 19806.

Cassazione penale, n. 8092 del 4/07/1987 in *Cassazione Penale*, 1989, pag.36.

Cassazione penale, 29/09/1987, in *Rivista Penale*, 1988, pag. 848.

Cassazione penale, sez. I del 13/06/1987 in *Cassazione Penale* 1988, pag. 1812.

Cassazione penale, del 26/11/1987, Trimboli, in *Rivista Penale*, 1989.

Cassazione penale, sez. I del 01/07/1988 in *Giustizia Penale*, 1989, Vol. II, pag. 535.

Cassazione penale,sez. I del 21/03/1989 in C.E.D. Cassazione .

Cassazione penale, n. 8864 del 27/06/1989 in *Cassazione Penale*, 1991, pag. 1042.

Cassazione penale, sez. VI del 13/07/1989 in *Cassazione Penale*, 1991, pag. 309.

Cassazione penale, sez. I del 03/10/1989 in *Cassazione Penale* 1991, Vol. 1, pag.744.

Cassazione penale, sez. I del 25/05/1990, in *Cassazione Penale* 1992, pag.300.

Cassazione penale,sez. VI,del 27/05/1991, in *Giurisprudenza Italiana*, 1993, vol. II, pag. 163.

Cassazione penale, sez. I,del 21/02/1992, in *Giustizia Penale*, 1992, Vol. II, pag. 428.

Cassazione penale, sez. I del 23/11/1992, in *Cassazione Penale*, 1995, pag. 45.

Cassazione penale, sez. I del 11/12/1992, in *Giustizia Penale*, 1994, Vol. II, pag. 258.

Cassazione penale, sez. I n. 4805 del 08/01/1993, in *Cassazione Penale*, 1995, fasc. I, pagg.11-13

Cassazione penale, sez. IV del 22/2/1993, in *Giustizia Penale*,19993, Vol. II, pag. 517, 629.

Cassazione penale, sez. I del 27/02/1993, in *Giurisprudenza Italiana* 1994, Vol. II,pag. 672.

Cassazione penale, sez. VI, n. 1793 del 03/07/1993, in *Rivista Penale* 1995, p. 649.

Cassazione penale, sez. I del 24/01/1994, in *Giustizia Penale*, 1994, Vol.II, pag.424.

Cassazione penale, sez. I del 18/03/1994 in *Cassazione penale* 1994, pag. 2685.

Cassazione penale, sez. VI del 10/05/1994 in *Cassazione Penale*, 1996, pag. 1124.

Cassazione penale sez. II n. 4342 del 14/10/1994, in CED Cassazione. Penale. 1994.

Cassazione penale, sez. I del 05/12/1994, in *Cassazione Penale* 1996, pag.77.

Cassazione penale, del 14/6/1995, in *Cassazione Penale* 1997, Vol. 3, pag.398.

Cassazione penale, sez. I n. 67 del 15/01/1997, in *Cassazione Penale,* 1998, pag. 803.

Cassazione penale,sez. I, n. 66 del 15/01/1997, Ciampà, in *Cassazione Penale*, 1998.

Cassazione penale, del 30/1/1997, in *Cassazione Penale,* 1998, pag.803.

Cassazione penale, sez. VI n.5500 del 30/03/1998, in C.E.D. Cassazione 1998.

Cassazione penale, sez. VI, n.468 del 30/03/1998, in Rassegna Avvocatura di Stato, 1999.

Cassazione penale, sez. V n. 10076 del 24/09/1998, in *Cassazione Penale* 2000, pag. 1946.

Cassazione penale n. 6239 del 26/3/1999, in C.E.D. *Cassazione Penale,* Rv.212810.

Cassazione penale, sez. V, n.12732 del 7/11/2000, in *Cassazione Penale*., 2002, pag. 1015.

Cassazione penale, sez. VI del 4/10/1999, in *Foro Italiano*, 2000, Vol. 123, n.3, pagg. 133-140.

Cassazione penale, sez. V, n. 12525 del 28/06/2000 in *Cassazione Penale* 2001, Vol. 10, p.2686.

Cassazione penale, sez. V, n. 4741 del 17/11/2000, in http://www.interlex.it/testi/cp4741.html/.

Cassazione penale n. 33717 del 17/9/2001, in C.E.D. *Cassazione Penale*, Rv. 2219921.

Cassazione penale, sez. I, n. 17027 del 25/03/2003, in *Cassazione Penale* 2004, pag. 2346.

Cassazione penale, sez. V del 24/11/2003, Russello, in *Foro Italiano*, 2005, n.6, pagg.323-332.

Cassazione penale, del 18/03/2004 in *Diritto Penale e Processo*, 2004, pag. 685.

Cassazione penale, sez. VI, n.26010 del 23/04/2004, in *Rivista Penale* 2005, pag. 1391.

Cassazione penale, sez. III, n. 8296 del 02/12/2004, in *Cassazione penale*, 2006, Vol. 5, pag.1819.

Cassazione penale, sez. II n. 2350 del 21/12/2004, in *Rivista Penale* 2006, pag. 92.

Cassazione penale, sez. II, n. 49691 del 28/12/2004 in *Diritto Penale e Processo*, 2005, n.5, pagg. 593-599.

Cassazione penale, sez. VI n. 12845 del 24/02/2005, in *Cassazione Penale* 2006, vol.4, pag. 1459.

Cassazione Sezioni Unite, n.33748 del 12/07/2005 in *Foro Italiano*, 2006, vol. II, pagina 86.

Cassazione penale, sez. I n. 39757 del 28/09/2005, in *Giurisprudenza Italiana* 2006, vol. 7, pag.1483.

Cassazione penale, sez. I n. 34043 del 11/10/2006, in *Rivista Penale*, 2006, pag. 663.

Cassazione penale, sez. III, n. 35521 del 06/07/2007, in C.E.D. Cassazione n. 237397.

Cassazione penale, sez. III, n.24263 del 10/05/2007, in C.E.D. Cassazione 2008.

Cassazione penale, sez. V, n. 46674 del 14/12/2007 in *Diritto dell'Internet*, 2008, n.3, pagg. 249-252.

Cassazione penale, sez. I., n 40552 del 20/10/2009.

Cassazione penale, sez. V n. 37370 del 07/06/2011, in CED Cassazione 2011.

Cassazione penale, sez. VI n. 3886 del 07/11/2011, in C.E.D. Cassazione 2011.

Cassazione penale, sez. III n.29899 del 09/06/2011, in *Guida al Diritto* 2011, numero 45, pag. 84.

Cassazione penale, sez. VI, n. 9117 del 16 /12/2011, in C.E.D. Cassazione 2012, Rv. 252386.

Cassazione penale, sez. III n. 8024 del 25/01/2012, in C.E.D. Cassazione 2012.

Cassazione penale, sez. II, n.22953 del 16/05/2012, in *Cassazione Penale* 2013, Vol.11, pag. 4078.

Cassazione penale, sez. II, n. 20451 del 03/04/2013, in C.E.D. Cassazione 2013.

Cassazione penale, sez. III n. 20921 del 14/03/2013, in C.E.D. Cassazione penale 2013.

Cassazione penale sez. VI, n. 50334 del 02/10//2013, in C.E.D. Cassazione Penale 2013.

Cassazione penale, sez. VI, n. 10866 del 06/03/2014 in C.E.D. Cassazione Rv. 259493.

Cassazione penale, sez. III numero 47249 del 13/05/2014 in *Diritto & Giustizia*, 2014, 18/11.

Cassazione penale, sez. VI,n. 4294del 09/10/2014,in *Rivista Penale* 2015, Vol.3, pag. 244.

Cassazione penale, sez. VI, n. 45168 del 29/10/2015, in C.E.D. Cassazione 2016.

Cassazione penale, sez. II n. 50338 del 03/12/2015, in *Cassazione Penale* 2016, Vol. 4, pag. 1704.

Cassazione penale, sez. I n. 1911 del 18/12/2015, in *Diritto & Giustizia*, 20/01/2016.

Cassazione penale, sez. III n.35578 del 21/04/2016, in C.E.D. Cassazione 2016 .

Cassazione penale, sez. V n. 34988 del 18/08/2016, in *Guida al diritto* 2016, n.38, pag.92.

Cassazione penale,sez. V, n. 20485 del 23/03/2018, in *Guida al diritto*,2018, n.26, pag.80.

Cassazione penale, sez. V, n. 1964 del 07/12/2018, in C.E.D. Cassazione Penale 2019.

Cassazione penale, sez. VI, n. 31908 del 14/05/2019, Rv. 276469-01.

Cassazione penale sez. II, n. 35141 del 13/06/2019, in *Cassazione Penale*, 2020, fasc.3, pag.1167.

Cassazione penale sez. III, n.37541 del 11/07/2019.

Cassazione penale, sez. III n. 11570 del 30/01/2020, in *Responsabilità Civile e Previdenza* 2020, Vol.4, pag. 1305.

Cassazione penale, sez. II, n. 28868 del 02/07/2020.

Cassazione penale, sez. VI n.17018 del 28/05/2020, in *Redazione Giuffrè* 2020.

Cassazione penale, sez. VI, n. 22516 del 18/06/2020, in *Redazione Giuffrè* 2020.

Cassazione penale, sez. II, n.36251 del24/11/2020, in C.E.D. Cassazione Penale 2021.

Cassazione penale, sez. V, n. 33874 del 05/07/2021, in C.E.D. Cassazione 2021.

Cassazione penale, sez. V n. 25251 del 12/02/2021, in *Redazione Giuffrè* 2021

Cassazione penale, sez. II n. 7839 del 12/02/2021, in C.E.D. Cassazione 2021.

Cassazione penale, sez. III n. 47436 del 09/11/2021, in *Guida al diritto* 2022, vol. 7.

Cassazione penale sez. IV, n.593 del 20/12/2022.

Cassazione penale sez. III, n.12525 del 01/03/2022.

Corte Costituzionale, n.19 del 1962, in *Giurisprudenza Costituzionale*, pag. 189.

Corte Costituzionale, n.65 del 1970; in *Giurisprudenza Costituzionale* 1970, pag. 955.

Corte Costituzionale, n. 199 del 1972, in *Giurisprudenza Costituzionale,* 1972, pag. 2218.

Corte d'appello di Ancona, n. 719 del 20/04/2021, in *Redazione Giuffrè* 2021.

Corte d'Appello di Catanzaro, sez. I del 2/2/1985 in *Cassazione Penale*, 1985.

Corte d'Appello di Palermo, n.1564 del 2/05/2003 in ArchivioAntiMafia.org.

Corte di Giustizia Europea, Causa C-176/03 del 13/09/2005, https://eurlex.europa.eu/legalcontent/IT/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A2005%3A542.

Tribunale Milano, 1/3/2001, in *Rivista Italiana di diritto e procedura Penale,* 2002, fascicolo 1, pagg. 316-368.

Tribunale Milano sez. IV, n.1972 del 12/04/2010 in: *Rivista del diritto Industriale* 2010, numero 4-5, vol.II, pagg.328 e ss; *Giurisprudenza di Merito* 2011, vol.1, pag.159.

Tribunale Milano, 28 /9/ 2007, in *Foro ambrosiano*, 2007, pag.325.

Tribunale Torino, n. 753 del 13/01- 9/02/2004, in *Guida al Diritto,* 2004, pag. 65.

Tribunale Siracusa, n. 229 del 19/06/2012, in *Giurisprudenza di Merito*, 2013, fasc.11, pag.2428.

Sitografia

4chan.org:https://4chan.org/

Archivio AntiMafia.org:https://www.archivioantimafia.org/

Centro Elettronico di Documentazione della Corte di Cassazione: https://www.italgiure.giustizia.it/

Collective Security Treaty Organization (CSTO): https://en.odkb-csto.org/

DigitCult - Scientific Journal on Digital Cultures: https://digitcult.lim.di.unimi.it/index.php/dc

Eur Lex (Sito ufficiale di raccolta della legislazione e giurisprudenza dell'Unione Europea): https://eur-lex.europa.eu/homepage.html?locale=it

Google AI: https://ai.google/ .

Google -Threat Analysis Group: https://blog.google/threat-analysis-group/

"Norton Cybercrime Report: The Human Impact", 2010: http://www.norton.com/cybercrimereport/

Portale del Consiglio d'Europa sulle azioni contro il Cybercrime:https://www.coe.int/it/web/portal/coe-action-against-cybercrime

Registro ufficiale documenti della Commissione Europea:https://ec.europa.eu/transparency/documents-register/

Società cooperativa sociale - Centro Studi l'Arcobaleno:http://www.arcobalenocooperativasociale.com/

Statistica di SurfShark.com sul Cybercrime: https://surfshark.com/

Stastista.com- Cyber crime& Security section: https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#insights

Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine:https://www.unodc.org/

UNICEF- Resarch & Reports: https://www.unicef.org/reports

Ringraziamenti

Questo elaborato mi ha permesso di esplorare delle prospettive completamente diverse da quelle che ho utilizzato abitualmente durante la mia carriera universitaria: non posso dunque non ringraziare in primo luogo la **Professoressa D. Provolo** per la sua immensa disponibilità, pazienza e capacità di ascolto dimostratami durante quest'ultimo anno accademico, qualità che spero un giorno di acquisire e poter maturare nella mia futura vita professionale .

Questi anni universitari sono stati per me i più belli e i più intensi della mia vita, nella gioia e nel dolore: devo perciò quindi ringraziare **la città di Padova,l'Università di Padova, la Scuola di Giurisprudenza, nonché tutti gli studenti, i docenti, gli assistenti, i professori e i dipendenti**, per tutte le lezioni- accademiche e di vita- che mi hanno fornito anche nel loro frettoloso camminare tra i corridoi e le strade.

Proseguo poi nel ringraziare quelle persone che mi sono sempre state accanto durante tutto questo periodo universitario (e non solo) senza il cui aiuto oggi non mi ritroverei a discutere questa tesi - la mia famiglia:

Devo quindi ringraziare (con statua in allegato) innanzitutto mia **Mamma Alba**, mio costante scontro e conforto: senza la tua passione per la vita e la tua capacità di scavare in fondo ad ogni mio singolo pianto e rabbia che non riuscivo ad esprimere appieno, non so se sarei laureata in un qualcosa che - per quanto sbuffassi spesso tra le pagine- sotto sotto mi piaceva. Ti voglio bene, e sono certa che il cammino che di recente abbiamo intrapreso insieme ci renderà molto più vicine l'una con l'altra.

Poi un'enorme grazie (anche a lei statua in allegato per il suo contributo invisibile in questo lavoro) va a mia sorella **Elena**. Sei una persona brillante, di cuore ed in gamba, e sono molto orgogliosa della donna che sei diventata: grazie per essere mia sorella. Spesso ti sei dovuta prendere tu il ruolo di persona responsabile in famiglia- anche nel nostro rapporto. So che ci vorrà tempo da parte tua ed impegno da parte mia, ma sappi che sono disposta ad ascoltarti e ad accoglierti al meglio per quello che sei, senza la tua corazza.

Altro ringraziamento (sempre con statuina inclusa) va al mio **papà Piero**: grazie al tuo immenso supporto, al tuo senso pratico e a tutte le sedute fatte insieme prima di ogni settembre per capire come orientarmi al meglio durante ogni singolo anno accademico, nonché per non avermi mai mollato sulla pianificazione delle mie attività e della mia vita.

Un pensiero va anche a mio **Zio Sandro**: grazie per il tuo immenso amore per la musica e per il tuo costante interesse nell'aggiornarti (anche a distanza) in quello che Elena ed io facciamo, riesco a sentire i tuoi applausi da Londra.

Mando anche un saluto ai miei **nonni:** quasi tutti voi ve ne siete andati a catena negli ultimi tre anni, ma ciò che mi avete lasciato - la schiettezza di **nonno Franco**, la dolcezza di **nonna Fanina,** l'allegria e serenità del **nonno Giovanni** e il non aver paura della propria lingua tagliente della **nonna Pinuccia** - non lo dimenticherò mai.

In questi anni universitari ho potuto cogliere appieno, per la prima volta, cosa voleva davvero dire amicizia, perciò non posso non ringraziare chi ha colorato con me (e so che continuerà a farlo) questi anni universitari. In ordine casuale, ringrazio:

Erica, per le sue pause tè in collegio e le sue sessioni di gossip da vera Presidentessa. Grazie per esser sempre stata pronta ad ascoltarmi quando sentivo il bisogno di sfogarmi e di avermi coinvolto in tutti i discorsi succosi del Collegio, grazie per avermi fatto sentire libera di essere me- con o senza gatti in giro.

La mia compagna di uscite serali (e non solo), **Martina S.**: tu ed Erica mi avete aiutato a calare quella maschera che avevo addosso da tanto tempo. Grazie per le nostre uscite delle 19 e ritorni alle 3 (se eravamo stanche), grazie per avermi fatto scoprire il bello dell'imprevisto e di avermi mandato … quando ne avevo bisogno.

Silvia, amica d'università e di viaggi: grazie per condiviso tutto con me, dai posti in aula studio ed i codici alle pizze e cucina cinese portata in serata per le nostre sessioni di ripetizione, nonché allo sfruttamento della tua macchina per i miei continui traslochi. Grazie per tutti i consigli di questi anni, ti devo tante birre tante quante le volte mi hai assicurato che ce la facevo.

Martina B., grazie per la tua incontenibile dolcezza e la tua spontaneità tra le austere e formali aule del Bo, e per la tua capacità di farmi sempre ridere, anche nei periodi in cui si era più stanche o stressate per gli esami.

Chiara, amica inaspettata del gruppo Padova'n Friends: grazie per la tua disponibilità ed apertura anche quando ancora non ci conoscevamo, la tua chiarezza di idee, nonché per tutta la tua vicinanza quando sei venuta a trovarmi in Sicilia. La tua forza e capacità di svegliarti presto sono per me una fonte d'ispirazione, grazie per esser diventata in poco tempo un così importante punto di riferimento per me.

Cecilia, grazie per esserti spinta oltre con me oltre al mero rapporto di colleghe universitarie ed essere andata a toccare nel profondo con me cose che potevi capire - amore per il crime compreso. So che, anche se rispondiamo entrambe tardi ai messaggi, ci sarò per te allo stesso modo in cui ci sarai tu. Sono ammirata dalla tua forza ed orgogliosa del cambiamento che hai avuto in questi ultimi anni, e non ho dubbi che la vita- accademica e non- ti riserverà bellissime sorprese nel futuro.

Marta, grazie per la tua bellissima sensibilità, grazie per tutti i posti dove siamo andati a mangiare insieme la cucina asiatica in Arcella e a tutte le referenze K-Pop. La tua sconvolgente capacità di metterti a nudo quasi immediatamente con una persona che ti sta solo simpatica per una persona celebrale ed estremamente selettiva come me è allo stesso tempo cosa curiosa e terrificante, per questo ai miei occhi sei un'amica ancora più preziosa di come ti vedi abitualmente.

Kristi, dedico due parole anche a te: so che non mi conosci bene tanto quanto Marti ed Erica, ma il parlare con te (quando ne avevi voglia) e le tue battute serali mi hanno permesso di abbattere tanti stupidi pregiudizi che avevo nei confronti del povero genere maschile, e di questo ti ringrazio molto- ma Eminem rimane molto meglio della trap.

Devo poi ringraziare la mia psicologa, la dott.ssa **L. Casetta**, per avermi guidato e per guidarmi nell'affrontare i miei lati <<avvelenati>> e l'immensa pazienza che ha mostrato con me in questi anni, grazie per la sua accoglienza e comprensione incondizionata nell'accompagnarmi passo dopo passo alla scoperta delle mie parti emotive- fin troppo a lungo trascurate.

Un enorme grazie va poi **all'Accademia de L'Inutile e a tutta la compagniadegli Inutili,** per la loro leggerezza in tre anni in cui ce n'era bisogno, per la conoscenza di persone splendide e la riscoperta della passione per il teatro. Sono passati un paio d'anni, ma continuo ad esser convinta di quanto la mia vita universitaria abbia acquisito una pienezza in più quando, inuna sera di Ottobre, decisi d'improvvisare sul momento con degli sconosciuti.

Mando anche un veloce ringraziamento alla squadra MMA della **Palestra Athena** e al loro Maestro, che ho abbandonato a malincuore l'anno scorso: grazie per avermi fatto comprendere che la rabbia e la forza non ti portano mai tanto lontano, ma è necessario soppesare e trovare l'equilibrio in ogni singolo movimento.

Un pensiero va anche alla mia OLP**Rossana Geraci** e ad i miei "colleghi"**volontari delServizio Civile Universale** di quest'anno (Ilenia, Andrea e per un pezzettino anche Sarah), per la loro immensa flessibilità nei turni mattinieri per permettermi di ultimare il mio lavoro di stesura, il loro interesse e le loro parole d'incoraggiamento durante le attività di Siracusa Città Educativa. Abbiamo cominciato da poco, ma è chiaro come il sole che, con la guida ferma di Rossana e le incredibili competenze di tutti voi, passeremo insiemeun anno che darà vita a tantissimi progetti - a cui non vedo l'ora di contribuire.

Infine, ringrazio me: grazie per avermi fatto accorgere, sotto lo strato della ragazza studiosa, che qualcosa non andava, grazie per non avermi mai mollato in tutto questo capitolo della mia vita.

Ma soprattutto,grazie per avermi fatto sentire in questi anni più volte le farfalle nello stomaco, facendomi intuire che – si, il percorso è lungo e difficile, sia all'Università che nella vita - ma che se qualcosa ti piace davvero e nel farlo ti mette dentro un fuoco dolce, in grado di riscaldarti il cuore, allora ne vale davvero la pena.