REATI INFORMATICI E CONCORSO DI NORME: COME L'EVOLUZIONE TECNOLOGICA INFORMA IL DIRITTO PENALE. IL CASO DELLE *BOTNETS*

dis CRIMEN articoli
2.12.2021

Tommaso Pietrella *

SOMMARIO 1. Note introduttive: diritto e criminalità informatica. — 2. La convergenza normativa nell'ambito dei reati informatici. Il caso delle *Botnets*. — 2.1. Concorso di reati nella *net* e con la *net*. — 3. Unicità e pluralità dell'azione in ambito informatico. — 4. Convergenza normativa, concorso apparente e reale di reati in materia di *Botnets*. — 5. Per un diverso attributo al principio del *ne bis in idem*. — 6. Reati informatici e nuova giustizia penale.

1. Note introduttive: diritto e criminalità informatica

Negli ultimi decenni del secolo scorso si è assistito ad una trasformazione epocale della società umana[1]. La rivoluzione informatica ha consentito la smaterializzazione della realtà fenomenica, introducendo nella storia universale oggetti privi di sostanza materiale[2], intangibili, componenti di una nuova e parallela realtà, quella virtuale. Il progressivo ampliamento degli strumenti informatici e la loro capillare diffusione hanno provocato, per quanto interessa ai nostri fini, uno sviluppo patologico dei sistemi di informatizzazione, ossia un'evoluzione delle pratiche criminose. Emergono, dunque, forme delinquenziali nuove, tanto per modalità di esecuzione, nella misura

* Dottorando di ricerca presso l'Università "La Sapienza" di Roma

[1] Importanti spunti di riflessione possono trarsi a tal riguardo in L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, 2017, in cui l'Autore illustra in che modo le radicali trasformazioni indotte dalle nuove tecnologie stiano tracciando la nuova linea di passaggio tra la storia e un'*iperstoria*. Cfr. anche: M. CASTELLS, *The rise of the network society*, Wiley-Blackwell, 2010, 2ª ed.; C. SARZANA DI SANT'IPPOLITO, *Criminalità e tecnologia: il caso dei "computer crimes",* in *Rass. penit. crim.*, 1979, n. 1, p. 53 ss.

[2] Basti pensare al basilare "dato" informatico, termine con cui si indica un'informazione elementare codificabile o codificata, meglio definito dalla Convenzione del Consiglio d'Europa sul *cybercrime* (Budapest, 2001) come: «*Any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*».

in cui sono agevolate dalla dematerializzazione dello "spazio" virtuale[3], quanto per beni materiali e giuridici coinvolti[4].

Nel processo evolutivo della cibernetica, un punto di svolta (ancora epocale) è segnato dall'apertura al pubblico, nei primi anni '90, di *Internet*[5], con ciò avendosi la transizione da una dimensione privata del "*personal computer*" e dei sistemi di elaborazione elettronica di dati, ad una dimensione aperta dei sistemi informatici, caratterizzata dalla loro globale interconnessione. L'avanzata integrazione tra sistemi di telecomunicazione e sistemi informatici ha, dunque, ampliato progressivamente i confini della categoria dei reati informatici, facendo emergere molteplici fenomenologie criminose[6].

Il termine "criminalità informatica" designa un concetto ampio e flessibile, non ancora cristallizzato in una definizione precisa e unanimemente accettata[7], che

[3] Si osserva che l'espressione "spazio virtuale", utilizzata per definire una realtà diversa da quella "reale", potrebbe essere impropria, dovendosi piuttosto parlare di una dimensione di "spazio" pluridimensionale e dinamica, globale. La pervasiva estensione della rete *Internet* e delle ICT (*Information and Communication Technologies*) ha coinvolto ogni ambito della vita umana, singola e collettiva, sicché, in questo mondo di iperconnettività, la realtà "reale" e quella "virtuale" vengono di fatto a sovrapporsi. Si rimanda, in particolare a L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI - S. CANESTRARI - A. MANNA - M. PAPA, *Cybercrime. Diritto e procedura penale dell'informatica*, UTET, 2018, p. 47.

[4] Cfr. L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutela*, in L. PICOTTI*, il diritto penale dell'informatica nell'epoca di internet*, CEDAM, 2004, p. 21 e ss.; ID., *Diritto penale e tecnologie informatiche*, p. 46; C. BLENGINO, *I reati informatici,* in M. DURANTE - U. PAGALLO, *Manuale di informatica giuridica e diritto delle nuove tecnologie*, UTET, 2012, p. 220 e ss.

[5] Cfr. L. PICOTTI*, Cybercrime e diritto penale*, in V. SELLAROLI - C. PARODI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Giuffrè, 2020, p. 712 e ss.

[6] In dottrina, diversi autori hanno evidenziato come tale accadimento storico segni l'evoluzione dei fatti criminosi da c*omputer crimes* (reati informatici) a *cybercrimes* (reati cibernetici). I termini, infatti, non sono sinonimi, ma esprimono due categorie distinte. I reati cibernetici si sviluppano e proliferano in conseguenza dell'accesso dei singoli ad una rete globale e della loro perdurante connettività. Implicano, dunque, la comunicazione virtuale o la diffusione di contenuti di ogni tipo nella rete. Si rimanda in particolare, *ex multis*, a L. PICOTTI, *Diritto penale e tecnologie informatiche*, p. 54 e ss.; ID. (a cura di), *Tutela penale della persona e nuove tecnologie*, CEDAM, 2013, p. 32 e ss.

[7] Cfr. C. PECORELLA, *Diritto penale dell'informatica*, CEDAM, 2006; C. SARZANA DI SANT'IPPOLITO, *Informatica, internet e diritto penale*, Giuffrè, 2010, 3ª ed., p. 54 e ss.; M. F. WEISMANN, *International Cybercrime: Recent Developments in the Law*, in R. D. CLIFFORD, *Cybercrime*, *Carolina Academic Press*, 2011, 3ª ed., p. 257; L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. econ.*, 2011, n. 4, p. 827 e ss. Una definizione di "criminalità informatica" o "*cybercrime*" non si rinviene neppure nella Convenzione di Budapest sulla criminalità informatica, avendo, il legislatore europeo, ritenuto di non cristallizzare il fenomeno in una formula definita, onde evitare il rischio di una sua celere desuetudine, stante il costante mutamento delle tecnologie e degli strumenti informatici.

ingloba al suo interno, quale grande contenitore, fenomeni di diversa natura. Si ritiene tuttavia possibile distinguere, nell'alveo dei fatti criminosi che possono essere commessi nel *cyberspace*, due diverse categorie di reati informatici[8]. Nella prima, quella dei "reati informatici in senso stretto", si è soliti includere «fattispecie legali che presentano espressamente, sul piano della loro formulazione letterale, elementi di tipizzazione descrittivi di modalità, oggetti, attività caratterizzati dalla o frutto della tecnologia informatica, vale a dire implicanti, connessi o relativi a procedimenti di elaborazione automatizzata di dati, secondo programmi informatici»[9]. Vi rientrano, ad esempio, i reati di: "accesso abusivo ad un sistema informatico o telematico" (art. 615-*ter* c.p.), "frode informatica" (art. 640-*ter* c.p.), "danneggiamento di informazioni, dati e programmi informatici" (art. 635-*bis* c.p.), *etc.* Essi rappresentano la tipizzazione di fatti nuovi, emersi con la progressiva diffusione delle nuove tecnologie ed estranei alle norme incriminatrici già esistenti[10].

Nella seconda categoria, i "reati informatici in senso lato"[11], rientrano fattispecie

[8] Sulla distinzione tra reati informatici "in senso stretto" e "in senso lato" si rimanda a: S. BRENNER, *Cybercrime Metrics: old wine, new bottles*?, in *Virginia J. L. & Tech.*, 2004, vol. 9, n. 13, p. 1 e ss.; L. PICOTTI, *Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l'informatique*, in *Revue internationale de droit pénal,* 2006, n. 3/4, p. 525 e ss.; F. R. FULVI, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in *dir. pen. e proc.*, 2009, n. 5, p. 639 e ss; P. GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, in *Rivista Elettronica di Diritto, Economia, Management*, 2010, n. 3, p. 95; G. D'AIUTO - L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, Giuffrè, 2012, p. 3 e ss.; R. FLOR, *Lotta alla "criminalità organizzata" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *www.dirittopenalecontemporaneo.it*, p. 4; C. PECORELLA, *Reati informatici*, in *Enc. Dir.*, 2017, p. 707 e ss.

[9] L. PICOTTI, *La nozione di "criminalità informatica"*, p. 845.

[10] Cfr. D. FONDAROLI, *La tutela penale dei «beni informatici»*, in *Dir. inform.*, 1996, n. 2, p. 295, ove è ben evidenziato come l'immaterialità dei beni informatici, quali dati, programmi e sistemi, su cui incidono le condotte criminose determina non poche difficoltà ove si debba dare applicazione a fattispecie incriminatrici già esistenti (es. furto, appropriazione indebita *etc.*), evidentemente incentrate sulla materialità degli oggetti.

[11] Secondo parte della dottrina, ai reati informatici in senso stretto si affiancano, non una, ma due diverse categorie, secondo la seguente tripartizione: 1) norme penali eventualmente informatiche; 2) norme penali informatiche in senso ampio; 3) norme penali informatiche in senso stretto. Il primo gruppo comprende tutte quelle disposizioni che, non tipizzando una specifica modalità di condotta, sono applicabili anche a fatti realizzati contro, o per mezzo, le tecnologie. Per norme penali informatiche in senso ampio si intendono, invece, quelle disposizioni che richiamano nel fatto tipico elementi informatici, pur essendo, in realtà, l'aggiornamento in chiave tecnologica di norme preesistenti. Si veda, sul punto, P. GALDIERI, *Teoria e pratica*, p. 95, il quale, a titolo esemplificativo, riconduce nella prima categoria il reato di estorsione (art. 629 c.p.); nella seconda, l'esercizio arbitrario delle proprie ragioni (art. 392 c.p.) che, a seguito della l. 547/93, può riferirsi anche alla violenza realizzata contro un bene informatico. Altrettanto interessante è la tripartizione formulata da D.S.

legali che, pur non tipizzando espressamente elementi di natura tecnico/informatica, comprendono anche i fatti criminosi commessi nel *cyberspace*, costituendo essi semplici forme di aggressione a beni giuridici già tutelati da norme incriminatrici comuni. Si pensi al reato di diffamazione, che può essere commesso mediante pubblicazione in *Internet* di contenuti offensivi della reputazione altrui; al reato di sostituzione di persona, integrato qualora siano utilizzate le generalità di una diversa persona per creare un falso account tale da provocare l'altrui errore; alle truffe che si consumano *online* previa pubblicazione di inserti decettivi.

A ben vedere, la divisione in due macrocategorie non risponde ad esigenze meramente classificatorie, ma riflette una differenza strutturale, nonché sostanziale, delle fattispecie coinvolte. Le tipologie riferite, infatti, chiamano in causa beni giuridici diversi[12], riflettono tratti criminologici differenti[13] e importano, ancora, diverse metodologie di tipizzazione delle norme incriminatrici.

Tale ultimo elemento necessita di un breve cenno di approfondimento. Volendo contrastare fenomeni legati al funzionamento delle tecnologie[14], il legislatore deve

---

WALL, *Maintaining Order and Law on the Internet*, in D.S. WALL, *Crime and the Internet*, Routledge, 2001, p. 167 e ss. e riproposta in B. SANDYWELL, *On the globalisation of crime: the Internet and new criminality*, in Y. JEWKES - M. YAR, *Handbook of Internet Crime*, Routledge, 2010, p. 46, secondo la quale possono distinguersi tre diverse sottocategorie di *e-crime*: 1) fattispecie criminose tradizionali che possono estendersi sino a ricoprire fatti commessi mediante computer e altri mezzi elettronici (es. lo spionaggio industriale); 2) fattispecie criminose tradizionali che sono amplificate per offesa o diffusione dall'utilizzo di mezzi elettronici e digitali (riciclaggio, terrorismo, pedopornografia); 3) fattispecie criminose che sono create *ad hoc*, ossia che tipizzano gli elementi della tecnologia (es. hackeraggio, *spamming*). In Italia, nella medesima direttiva, si veda F. MUCCIARELLI, *I computer crimes nel disegno di legge 1657/1984*, in *Riv. it. dir. proc. pen.*, 1985, n. 3, p. 785 e ss.

[12] Si rimanda, ancora, a L. PICOTTI, *Sistematica dei reati informatici*, p. 21 e ss.; ID., voce "Reati informatici", in *Enc. giur.*, Agg., VIII, Roma, 2000; G. PICA, voce "Reati informatici e telematici", in *Dig. pen.*, Agg., IV, Torino, 2000, p. 521 e ss.; C. PECORELLA, *Diritto penale dell'informatica*, cap. I; F. RUGGIERO, *Ciberspazio e diritto penale: il problema del bene giuridico*, in *Riv. pen.*, 2001, n. 3, p. 213 e ss.

[13] Cfr. C. SARZANA, *Informatica, internet e diritto penale*, p. 59.

[14] Laddove l'interpretazione giurisprudenziale non ha potuto utilizzare le fattispecie esistenti, stante i principi basilari di legalità penale e il divieto di analogia *in malam partem*, è bastato al legislatore aggiornare in chiave tecnologica le norme penali preesistenti, inserendovi elementi di informatica. Così, ad esempio, se la legge n. 547 del 1993 non avesse specificato che si ha "violenza sulle cose" "allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico", il reato di cui all'art. 392 c.p. si sarebbe difficilmente potuto applicare in tali casi, vista la materialità cui rimanda il concetto di "cosa". Non sono mancati, tuttavia, percorsi ermeneutici che hanno ritenuto possibile interpretare in senso evolutivo il termine "cosa" così includendovi anche i programmi installati in dispositivi informatici. Si veda, ad esempio, Tribunale Torino, 12 dicembre 1983, in *Giur. merito*, 1984, p. 1173 e ss., a mente del quale: «Pone in essere il delitto di cui all'art. 392 c.p. colui il quale, in qualità di

fare i conti con modalità, oggetti e comportamenti di natura prettamente informatica e implicanti processi calcolatori e automatizzati di sistemi informatici, ossia elementi tecnici difficili da trasporre sul piano normativo. Il rischio, infatti, è che l'individuazione di particolari modalità di condotta o realizzazione di evento, volte a dare veste giuridica a fatti criminosi riscontrati in ambito tecnico-informatico, possa risultare nel concreto una tecnica di normazione inefficace. Il costante aggiornamento delle tecnologie impiegate, il mutamento degli usi che se ne possono fare, potrebbero infatti far cadere in rapida desuetudine le norme incriminatrici di settore, insuscettibili di essere aggiornate al passo dello sviluppo tecnologico.

Per tali ragioni, sì è scelto di adottare una tecnica di tipizzazione che, pur impiegando nuove terminologie, non si concentra sulla tecnologia utilizzata, ma si focalizza più in generale sulle modalità della condotta, sulle finalità perseguite o, ancora, sugli eventi realizzati[15]. Lo strumentario di diritto sostanziale[16] adottato nel

dipendente di una società elaboratrice di programmi elettronici, ritenendo di esercitare un proprio diritto, sottrae dall'elaboratore di un'azienda parte di uno di tali programmi, precedentemente concesso in uso alla medesima, sempre che l'attività dell'agente abbia determinato una modificazione tale del programma stesso, da renderlo inutilizzabile secondo la sua normale destinazione». Questo indirizzo giurisprudenziale è stato recentemente confermato da Cass. pen., sez. II, del 10 aprile 2020 (ud. 07/11/19) n. 11959, che ha enunciato il seguente principio di diritto: «I dati informatici (*files*) sono qualificabili cose mobili ai sensi della legge penale e, pertanto, costituisce condotta di appropriazione indebita la sottrazione da un personal computer aziendale, affidato per motivi di lavoro, dei dati informatici ivi collocati, provvedendo successivamente alla cancellazione dei medesimi dati e alla restituzione del computer "formattato"». In tal caso, la Suprema Corte giustifica il proprio intervento estensivo richiamandosi ad un'interpretazione "logico-sistematica", e quindi non "analogica", delle fonti di rinvio. Tale ermeneutica non convince del tutto e il dubbio che la Corte abbia valicato gli stretti limiti della legalità penale non appare certo fugato.

[15] Sul punto si rimanda a E. ALBAMONTE, *Il reato informatico nella prassi giudiziaria: le linee giuda internazionali per il contrasto ai nuovi fenomeni criminali*, in *Rivista Elettronica di Diritto, Economia, Management*, n. 3, 2013, p. 146, il quale, tra l'altro, analizza in modo dettagliato le prassi criminose di maggior rilievo, come riscontrate nella prassi giudiziaria.

[16] In tema di evoluzione normativa, la scelta del legislatore è stata quella di non dedicare alla criminalità informatica un corpo normativo autonomo ovvero un esclusivo titolo all'interno del codice penale. La normativa in materia di criminalità informatica, infatti, è il frutto di molteplici interventi legislativi, fortemente condizionati da indicazioni di fonte sovranazionale. Sulla spinta delle Raccomandazioni del Consiglio d'Europa (in particolare la n. R (89) 9 – in materia di criminalità informatica - e n. R (95) 13, relativa a questioni procedurali) il legislatore ha approvato la legge 23 dicembre 1993, n. 547 ("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"), con la quale ha introdotto all'interno del codice nuove fattispecie delittuose (gli artt. 615-*ter*, *quater* e *quinquies*, 617-*quater*, *quinquies* e *sexies*, 635-*bis*, 640-*ter*, 623-*ter*) e modificando le fattispecie esistenti con riferimento ai beni informatici (ad esempio l'art. 392 c.p.). Ulteriori modifiche alla legislazione penale sono state poi apportate dalla legge 18 marzo 2008 n. 48, di ratifica della Convenzione di Budapest del 2001 (sono stati inseriti gli artt. 495-

nostro sistema penale[17], sembra, quindi, in grado di apprestare strumenti di qualificazione giuridica sempre attuali. Al contempo, tale tecnica di normazione rischia di ingenerare un incontrollato vortice di criminalizzazione, che non consente di inquadrare singoli fatti materiali entro un'unica fattispecie incriminatrice. La formulazione *latu sensu* generica dei precetti penali[18] fa sì che l'unitarietà del fatto materiale non si riproduca, quasi mai, sul piano giuridico, ove l'ampia portata delle fattispecie incriminatrici rende possibile la sussunzione di un solo accadimento storico-fattuale entro più cornici edittali.

Ci si chiede allora se l'adozione di una particolare tecnica di tipizzazione normativa giustifichi, nel settore dell'informatica, una diversa applicazione degli istituti di diritto penale. Il rischio di un'incontrollata superfetazione nelle

bis, 635-*ter*, *quater* e *quinquies*, 640-*quinquies*), per effetto della quale si è altresì prevista la responsabilità anche degli enti per un'ampia serie di reati informatici. Interventi legislativi successivi hanno poi introdotto ulteriori modifiche al codice penale, prevedendo, ad esempio, nuove aggravanti per i delitti di addestramento ad attività con finalità di terrorismo anche internazionale, di istigazione a delinquere o di atti persecutori, quando i fatti siano commessi attraverso strumenti informatici o telematici (novità introdotte dal decreto-legge n. 5 del 2017 e dal decreto-legge n. 93 del 2013). Ulteriori disposizioni si trovano al di fuori del sistema codicistico (ad esempio nel D. Lgs. n. 196 del 2003 o nella legge 22 aprile 1941, n. 633). Per una più specifica ricostruzione degli interventi normativi si rimanda a R. FLOR, *Cyber-criminality: le fonti internazionali ed europee*, in A. CADOPPI - S. CANESTRARI - A. MANNA - M. PAPA, *Cybercrime*, p. 97 e ss.

[17] Le cose non differiscono molto per gli altri ordinamenti giuridici, in quanto la tecnica normativa impiegata dal legislatore italiano riprende formule e modalità adottate nella Convenzione di Budapest del 2001. Si ritiene, a tal proposito, che l'utilizzo di categorie ampie e formulazioni generiche sia del tutto in linea con la natura giuridica di un trattato internazionale, posta la pluralità degli ordinamenti nazionali in cui tale convenzione è volta a produrre effetto. Ci si chiede, tuttavia, se anche il legislatore nazionale, calando il dettato normativo in un sistema chiuso e particolare, avrebbe dovuto impiegare una diversa e più specifica formulazione.

[18] A titolo esemplificativo, si assuma a paradigma il reato di cui all'art. 615-*ter* c.p., il quale risulta integrato in una vastità di casi, del tutto disomogenei tra loro. La fattispecie, infatti, copre tanto il caso di una moglie (la curiosità è un sostantivo femminile, perciò si consenta di ipotizzare un soggetto agente di sesso femminile), che a seguito della separazione dal marito e al suo allontanamento dalla casa coniugale, acceda all'account di posta elettronica di quest'ultimo, riuscendovi grazie alla precedente memorizzazione della *password* di accesso sul computer di casa o conoscendo, ella, al tempo della relazione coniugale, le credenziali d'accesso del marito (così: Cass. pen., sez. V, 2 ottobre 2018, n. 2905). Del medesimo titolo, risponde evidentemente anche il c.d. *hacker* professionista che, grazie a conoscenze e abilità altamente specializzate, inocula un *virus* in sistemi informatici per averne accesso (così: Cass. pen. sez. V, 30 maggio 2017, n. 48370). Pur essendo compresi nel medesimo tipo delittuoso, non c'è dubbio che i due casi siano riferibili a fenomenologie interamente differenti, anche solo dal punto di vista della condotta, ossia prescindendo dalla finalità per cui i due sono entrati nel sistema informatico e dall'evento, dannoso o pericoloso, conseguente all'introduzione abusiva. Assimilare sullo stesso piano fenomeni di natura tanto diversa, potrebbe avere effetti controproducenti in tema di politica criminale ed efficacia della risposta sanzionatoria.

qualificazioni giuridiche, strettamente conseguenziale alla peculiare formula di normazione prescelta, potrebbe allora legittimare, almeno in tale ambito, una diversa operatività dei criteri e dei principi regolatori del concorso di norme. E in tal senso il principio del *ne bis in idem*, attorno al quale si sviluppa la materia del concorso di norme, in effetti, ben si presta a porre rimedio al *vulnus* riferito. Del resto, sulla scorta dell'evoluzione dottrinale e, ancor di più, di quella giurisprudenziale che negli ultimi anni ha interessato l'elaborazione teorica e l'applicazione pratica del *ne bis in idem*, si intravedono oggi buone possibilità per attribuire al principio un volto nuovo[19], capace di adattare – quale clausola elastica – l'intero sistema penale alle criticità che il tecnicismo informatico pone in ambito giuridico.

2. La convergenza normativa nell'ambito dei reati informatici. Il caso delle *Botnets*

Sebbene sia stata già anticipata la sua conclusione, vale la pena fare un passo indietro e mettere in chiaro i termini della questione. Avendo il legislatore adottato una modalità di tipizzazione normativa che non richiama le tecnologie impiegate, così selezionando, quali elementi tipici delle fattispecie, determinate condotte, eventi e finalità, si assiste – in questo ambito – ad una continua interferenza tra norme, insuscettibile di riprodurre sul piano giuridico quell'unitarietà che, nella sostanza, caratterizza diversi fatti delittuosi di natura informatica. Tra le diverse tecnologie e prassi criminali sino ad oggi riscontrate, l'analisi e lo studio delle "botnets" può essere assunto a paradigma della questione di cui si tratta, in quanto la sua creazione e il suo utilizzo da parte dell'autore criminale coinvolge la quasi totalità delle fattispecie criminose del settore.

Una "botnet" (o "Bot Network") è una rete formata da dispositivi informatici collegati ad *Internet* e infettati da *virus* o *malware*, controllata da un'unica entità, il c.d. *botmaster* (o anche *command and control centre*[20]), che tramite l'inoculazione del programma malevolo (che può avvenire secondo le più svariate modalità, ossia

[19] Sul valore precettivo del *ne bis in idem*, sul suo significato intrinseco e i suoi risvolti applicativi, si consenta un rinvio a T. PIETRELLA, *Illecito e sanzione: il valore precettivo del ne bis in idem oltre il diritto penale*, in *JUS – Online*, 2020, n. 6, p. 129 e ss., reperibile alla URL: https://jusvitaepensiero-.mediabiblos.it/news/allegati/6%20-%20Pietrella.pdf.

[20] Un server di *Command and Control* (C&C) è il *server* dal quale dipende l'intero funzionamento di una *botnet*. Opera mediante l'invio di file di configurazione a computer e dispositivi delle ignare vittime, contenenti le più svariate istruzioni da seguire, oppure aggiornando il *malware* già inoculato alle versioni più recenti, o ancora inviando direttamente ai computer infettati comandi da remoto.

attraverso campagne di *spamming*, mediante l'utilizzo di *banner* o di domini malevoli, *etc.*) è in grado di comandare il sistema da remoto[21] e impartire ordini ai dispositivi della rete fruttando i canali IRC[22]. I dispositivi che compongono la *botnet* sono per questo chiamati *bot* (da roBOT) o anche solo *zombie*.

I controllori della *botnet* possono in questo modo sfruttare i sistemi compromessi per scagliare attacchi del tipo *distributed denial of service* (*DDoS*)[23] contro qualsiasi altro sistema in rete oppure compiere altre operazioni illecite, quali spionaggio, atti di terrorismo, estorsioni, traffici di organizzazioni criminali, *etc.* Non necessariamente il soggetto che controlla la *botnet* è il suo stesso creatore. Attraverso il c.d. *deep web*[24], infatti, sono facilmente fruibili tutti gli strumenti a disposizione dei

[21] Cfr. la linea guida adottata dalla *Cybercrime Convention Committee* sulle "botnets" n. 2 (2013 – 6 E Rev), reperibile online alla URL: https://rm.coe.int/CoERMPublicCommonSearchServices/-DisplayDCTMContent?documentId=09000016802e7094.

[22] I canali IRC (*Internet Relay Chat*) rappresentano la prima forma di comunicazione istantanea su Internet, che consente sia la comunicazione diretta fra due utenti (si pensi ad una chat di Skype) che il dialogo contemporaneo di interi gruppi di persone in stanze di discussione (ad esempio un "gruppo" di WhatsApp).

[23] La Linea guida T-CY n. 5 (2013 – 10 E Rev), adottata con delibera della nona Plenaria del 5 giugno 2013 (reperibile online alla pagina https://rm.coe.int/09000016802e9c49), definisce i cosiddetti *DoS* (*Denial of service)* come malfunzionamenti dovuti ad un attacco a causa del quale si esauriscono deliberatamente le risorse di un sistema informatico che fornisce un servizio (ad esempio un sito web), fino a renderlo non più in grado di erogare il servizio. Una variante di tale metodologia criminale è il *DDoS* (*Distributed Denial of Service*), dal funzionamento identico ma realizzato utilizzando numerose macchine attaccanti che insieme costituiscono una *botnet*. Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito ad un *server Web*, FTP o di posta elettronica saturandone le risorse. Infatti, l'invio di un numero superiore di e-mails rispetto a quelle che il *server* del servizio di posta elettronica possa ricevere, oppure l'invio di richieste non corrette o di richieste superiori a quelle che un sistema computerizzato possa simultaneamente elaborare paralizza il *server* attaccato, impedendogli di erogare il servizio che prima realizzava.

[24] A differenza dei comuni utenti, i criminali sfruttano spazi non rintracciabili attraverso motori di ricerca e non facilmente accessibili, comunemente chiamati *deep web*. All'interno di questo spazio sommerso, i siti che lo compongono non sono raggiungibili con i normali browser (i programmi per navigare su *Internet*, come Internet Explorer, Firefox o Safari) perché le loro pagine non sono indicizzate dai motori di ricerca. Tra l'altro, nel *deep web* si trovano anche siti accessibili solo attraverso *Virtual Private Network* (VPN), cioè collegamenti diretti e criptati tra due computer. Per accedere al *deep web* occorrono software creati per permettere la navigazione in anonimato, ossia in grado di celare l'indirizzo IP.

Il commercio illegale all'interno del *deep web* si basa, per la maggior parte, sull'utilizzo del *Bitcoin* come valuta, attraverso la quale vengono acquistati e venduti sostanze stupefacenti, armi, materiale pornografico *etc.* Essendo una valuta virtuale e crittografata, il *Bitcoin* permette l'anonimato sia dell'acquirente sia del venditore, così che rappresenta la moneta di scambio ideale per questo tipo di traffici. Cfr. F. ZAPPA, *La criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo*, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2014, p. 7.

cyber criminali che, per esempio, possono acquistare o, addirittura, solo affittare *botnets* per realizzare attacchi del tipo *DDoS*, campagne pubblicitarie o altre violazioni di sistemi[25].

Come anche previsto dalle linee guida adottate in seno alla Convenzione sul *cybercrime*, la creazione e l'utilizzo di una *botnet* integrano molteplici disposizioni incriminatrici: accessi abusivi ai sistemi, intercettazioni e danneggiamenti di dati e sistemi informatici, l'acquisizione, a seconda della tipologia di *malware* inoculato, di dati personali, *password* e altri codici di accesso, frodi informatiche, *etc.*

Al fine di valutare le fattispecie rilevanti, è possibile suddividere il fenomeno in tre diverse fasi: la creazione della rete, mediante l'infezione dei sistemi[26]; la fase di

[25] Per avere contezza del fenomeno, può giovare un richiamo a quella *botnet* di fama mondiale soprannominata "Avalanche", smantellata nel novembre del 2016 grazie alla cooperazione di numerose agenzie investigative, nazionali e di istituzioni sovranazionali. Si stima che il numero di dispositivi attaccati attraverso diverse famiglie di *malware* avesse raggiunto una media di un milione alla settimana, determinando l'insorgere di un network di dispositivi infetti di vastissime dimensioni, con una dislocazione in più di 180 paesi. In base al tipo di *malware* inoculato nei dispositivi delle vittime, i controllori della *botnet* erano in grado di commettere: estorsioni e danneggiamento di sistemi informatici; intercettazioni di comunicazioni; detenzione abusiva di codici di accesso; frodi informatiche e accessi abusivi. Tra i *virus* di maggior pericolo di cui si è avvalsa la *botnet* è possibile distinguere: *Windows-encryption Trojan horse* (WVT) e *Nymaim*, *malware* di tipo *ransomware*, in grado di criptare i dati presenti sul PC della vittima e renderli, quindi, non più utilizzabili, utilizzati per costringere la vittima a pagare una somma di denaro, in forma di riscatto, per la loro decriptazione. *URLzone*, *Bugat, Vawtrak* (noto anche come *Neverquest*) e *Tinba* (noto anche come *TinyBanker*), *malware* di tipo *banking trojan*, programmati per carpire credenziali a servizi di *online banking*. *NewGOZ* (o anche *GameOverZeuS*), *VM-ZeuS* e *Citadel*, *malware* di tipo *keylogging*, atti a sottrarre informazioni riservate (es. password o credenziali d'accesso a servizi bancari), memorizzando i caratteri digitati sulla tastiera del computer infettato, o anche di tipo *RAT*, in grado di far acquisire all'autore il controllo da remoto del PC della vittima. Infine, *Andromeda* (noto anche come *Gamarue*): *malware* di tipo *trojan*, inviato principalmente attraverso campagne di *phishing*. La *botnet* "Avalanche" era utilizzata come piattaforma di lancio, a livello globale, di massivi attacchi informatici. Si ritiene che, solo in Germania, "Avalanche" abbia causato dal 2009 un danno pari a 6 milioni di euro, indirizzando una serie continuata di attacchi ai sistemi bancari digitalizzati. Su scala mondiale, le perdite monetarie dovute all'utilizzo della *botnet* sono invece stimate in migliaia di milioni di euro.

Si stima, a livello mondiale, che tra il 16-25% circa dei computer connessi alla rete sia, all'insaputa dei loro proprietari, connesso ad una rete *botnet*. Cfr. S.S.C. SILVA - R.M.P. SILVA - R.C.G. PINTO - R.M. SALLES, *Botnets: A survey*, in *Computer Networks*, 2013, vol. 57, n. 2, p. 378 e ss.

[26] Secondo l'ampia definizione valsa nella giurisprudenza di legittimità, per sistema informatico si intende: «Un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (*bit*), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente»

utilizzo, in cui i programmi malevoli installati lavorano nelle macchine facendone dei *bots*; l'esecuzione del piano criminoso, ove la rete costruita viene impiegata per la realizzazione di attività altrettanto illecite.

Nella fase di infezione, la prima norma ad avere rilievo applicativo è la fattispecie delineata dall'art. 615-*quinquies* c.p. "diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico": il controllo dei dispositivi delle vittime avviene previa diffusione di *malware* o *virus*[27], che vengono introdotti subdolamente all'interno della macchina delle vittime. Il *malware* o *virus*, una volta che è riuscito a penetrare nel sistema informatico attaccato, altera inevitabilmente i dati o i programmi contenuti in quel sistema, compromettendone le funzionalità. I *software* malevoli, infatti, altro non sono che istruzioni di un programma codificate in linguaggio macchina o in linguaggio di programmazione sotto forma di codici eseguibili. L'inoculazione del *virus* nel dispositivo della vittima, seppure non si possa astrattamente prescindere dalla natura del programma malevolo utilizzato, è nella maggior parte dei casi idonea a realizzare danneggiamenti informatici *ex* artt. 635-*bis* e 635-*quater* c.p.[28].

(così Cass. pen., n. 3067 del 1999, Riv 214945, richiamata anche da Cass. pen., sez. II, 6 marzo 2013, (ud. 06/03/2013, dep. 22/03/2013), n. 13475). Vanno dunque ricompresi nel concetto di sistema informatico «non solo i tradizionali elaboratori di dati (*computer*), ma anche i dispositivi elettronici più evoluti (*smartphone*, *tablet*), nonché ai più evoluti sistemi basati sulla tecnologia IoT, che consente di interconnetter le "cose", meglio gli oggetti intelligenti (*smart objects*) ad Internet».

[27] I *malware* riescono ad essere installati nei dispositivi delle vittime a causa dell'inadeguatezza dei c.d. *firewall* o *antivirus* presenti o, ancora, a causa di falle nella sicurezza. Vengono diffusi, in modo prevalente, tramite *Internet* secondo plurimi schemi: attraverso messaggi di posta elettronica, creati mediante tecniche di *social engineering* per incoraggiare il destinatario ad aprire il *file* allegato che nasconde un *malware*. Una volta aperto quest'ultimo, il codice *malware* si installa sul dispositivo. Mediante collegamenti URL dannosi nel testo di un'e-mail, che indirizzano la vittima a pagine web di un sito compromesso e contenente il codice malevolo. Tramite *drive-by download*, allorquando l'inoculazione del *malware* avviene visitando un sito contenente codice malevolo o tramite reindirizzamento alla pagina del sito tramite un annuncio malevolo (*malvertising*). Ancora: tramite dispositivi USB infetti; mediante intrusioni dirette nelle reti locali o un *plug-in Flash* non aggiornato o non configurato correttamente nel browser dell'utente; tramite *download* di versioni demo, *trial* e *freeware* di altri *software* o videogiochi, di *toolbar* per i *browser*, di finti *antivirus* e *tool* di rimozione, di applicazioni per dispositivi mobile scaricate da *app store* non ufficiali e di qualsiasi altro materiale scaricabile da *Internet* in cui possono essere nascosti *malware* e *virus*.

[28] L'art. 635-*quater* c.p. prevede quale condotta penalmente rilevante il danneggiamento di un sistema informatico, se realizzato mediante una delle modalità previste dall'art. 635-*bis*, ossia: distruzione, cancellazione, deterioramento o alterazione o soppressione di informazioni, dati o programmi informatici altrui. La formulazione appare infelice. Le modalità descritte dall'art. 635-*bis* c.p., infatti, possono di per sé essere considerate forme di danneggiamento di sistemi informatici, in quanto comportano l'elaborazione di dati e l'esecuzione di operazioni non necessarie al sistema

Pur variando nel tipo, quando un *malware* è programmato per consentire, ad un soggetto estraneo, il controllo del dispositivo da remoto, viene poi in rilievo la fattispecie di "Accesso abusivo a sistema informatico" (art. 615-*ter* c.p.), specialmente nella forma aggravata, ove al danneggiamento dei sistemi e dei dati ivi contenuti è equiparata anche la loro semplice alterazione o modificazione[29]. L'acquisita possibilità di accedere al sistema infettato può, in alcuni casi, consentire all'autore dell'illecito l'acquisizione fraudolenta di dati e informazioni riservate ivi memorizzate. Vengono dunque il rilievo i reati posti a tutela della riservatezza, l'art. 167 D.lgs. 30 giugno 2003, n. 196 ("trattamento illecito di dati personali"), o prodromici ad assicurare, in via anticipata, il domicilio informatico, come l'art. 615-*quater* c.p. (nel caso in cui dall'accesso al dispositivo infettato derivi il procacciamento di *password* o codici d'accesso per *home-banking*, *account*, *etc.*).

Una volta che il *malware* è stato installato nel sistema informatico della vittima e che il c.d. *botmaster* ha assunto il suo controllo, il programma malevolo può provocare poi una alterazione dei flussi di comunicazione informatica, sussumibile nel reato di cui all'art. 617-*quater* c.p., "Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche". Infatti, se il dispositivo infettato è connesso ad *Internet*, il *malware* può essere in grado di modificare i comportamenti comunicativi tra il *client* e il *server*[30] nel momento dinamico della loro trasmissione, frapponendosi tra la prima componente, che interroga il sistema centrale, e la seconda, che gli restituisce le informazioni richieste, così intercettando, impedendo o

(rallentandone la velocità, consumandone l'energia *etc.*) o/e dannose al suo stesso funzionamento. Si evidenzia, in dottrina, che il reato previsto all'art. 635-*quater* c.p. si riferisce esclusivamente a fatti "violenti" di danneggiamento, ove sia riscontrabile un evidente deterioramento delle capacità del sistema informatico. In materia, si rimanda a: I. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. e proc. pen.*, 2012, n. 1, p. 204 e ss.

[29] Si segnala, in materia, un orientamento più rigoroso, che non ravvisa nell'infezione di un sistema la sua inevitabile modificazione o alterazione. All'inoculazione di un *virus*, si dice, non conseguirebbe *ipso facto* un danneggiamento dei sistemi o dei dati, dovendo piuttosto «ritenersi che "alterare" un programma significhi anche manipolarlo in modo che compia azioni non volute dall'utente, ovvero modificarne i parametri di funzionamento, anche secondo opzioni e possibilità previste nel programma stesso, contro la volontà dell'utilizzatore». Corte d'Appello di Bologna, sez. II, 27 marzo 2008, n. 369.

[30] In informatica, il termine *client* individua una determinata componente *hardware* o *software* che accede alle risorse o ai servizi erogati da un'altra componente, il *server*, il quale, a sua volta componente *hardware* o *software*, fornisce i dati richiesti da una o più *client*. In altre parole, un *server* non è altro che un computer e/o un programma in grado di rispondere alle richieste fatte da altri computer e/o da altri programmi. Questo semplice modello di scambio "uno ad uno" è, con diverse varianti, alla base del funzionamento del *web*.

interrompendo, a seconda della tipologia di *virus* utilizzato, le comunicazioni tra sistemi[31]. Ci si chiede poi se possa trovare talora applicazione anche il reato previsto dall'art. 617-*quinquies* c.p., "Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche", figura delittuosa molto simile a quella prevista dall'art. 615-*quinquies* c.p.[32].

L'inoculazione del *virus*, alla luce degli eventi che è suscettibile di provocare, sembra integrare anche il reato di "frode informatica" di cui all'art. 640-*ter* c.p. Non c'è dubbio, infatti, che l'infezione di un dispositivo tramite *malware* e *virus* si sostanzi tanto nell'alterazione del funzionamento di un sistema informatico o telematico[33] quanto in un intervento su dati, informazioni o programmi ivi contenuti. Il danno, poi, che il sistema della vittima patisce in conseguenza dell'attacco informatico è

[31] Dalla collocazione sistematica della norma tra i "delitti contro la inviolabilità dei segreti" potrebbe desumersi che la condotta incriminata si rivolga unicamente a comunicazioni tra soggetti, che si scambiano, tramite il linguaggio informatico o telematico, contenuti, idee, pensieri. La giurisprudenza, invece, ha fatto ampio utilizzo della fattispecie, così da comprendere anche le comunicazioni di dati informatici. Si veda a tal proposito Cass. pen., sez. V, 9 ottobre 2020, (ud. 09/10/2020, dep. 12/01/2021), n. 869, ove è stata esplicitamente disattesa la tesi difensiva secondo la quale l'art. 617-*quater* c.p. è volta a sanzionare la captazione dei soggetti tra i quali intercorre la comunicazione. Così anche L. SCOPINARO, *Internet e reati contro il patrimonio*, Giappichelli, 2007, p. 216: «L'art. 617-quater c.p., d'altro canto, punisce chiunque «impedisce» oppure «interrompe» «comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi», cioè, fra l'altro, flussi di dati intercorrenti fra un sistema e l'altro quando i sistemi sono interconnessi l'uno con l'altro».

[32] Raffrontando le due fattispecie emerge un dato importante: mentre il reato previsto all'art. 615-*quinquies* si applica alla diffusione di "apparecchiature, dispositivi o programmi informatici", la fattispecie prevista dall'art. 617-*quinquies*, invece, fa esclusivo riferimento alle "apparecchiature". Il mancato richiamo ai dispositivi o programmi informatici da parte della seconda norma sembrerebbe avvalorare una rigorosa ermeneutica, a mente della quale è penalmente rilevante solo l'installazione di supporti fisici di tipo *hardware*. La giurisprudenza di legittimità, tuttavia, sembra comprendere nel termine "apparecchiature" anche programmi informatici. Così, Cassazione pen. sez. V, 18 marzo 2019, (ud. 18/03/2019, dep. 05/04/2019), n. 15071, a parere della quale: «Al lume di tale autorevole interpretazione del diritto vivente, non è possibile dubitare dell'inclusione dei programmi informatici denominati "spy - software" nella categoria degli "apparati, strumenti, parti di apparati o di strumenti" diretti all'intercettazione o all'impedimento di comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone, di cui all'art. 617-*bis* c.p., comma 1, venendo in rilievo una categoria aperta e dinamica, suscettibile di essere implementata per effetto delle innovazioni tecnologiche che, nel tempo, consentono di realizzare gli scopi vietati dalla legge».

[33] In modo particolare se si accoglie una definizione ampia di "alterazione". Sostiene, ad esempio, un orientamento giurisprudenziale, che: «Per alterazione deve intendersi ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei suddetti dati e, quindi, sia sull'*hardware* che sul *software*. In altri termini, il sistema continua a funzionare ma, appunto, in modo alterato rispetto a quello programmato». Così Cass. Pen., sez. II, 1 dicembre 2016, (ud. 01/12/2016, dep. 23/12/2016), n. 54715; Cass. Pen., sez. II, 24 febbraio 2011, (ud. 24/02/2011, dep. 11/03/2011), n. 9891.

direttamente proporzionale al profitto che il soggetto agente trae dall'utilizzo della *botnet*, tramite la quale l'utilizzatore è in grado di realizzare lo scopo criminoso perseguito. Occorre infine valutare se l'accesso e il controllo da remoto del dispositivo infettato da parte del c.d. *botmaster* consenta *ipso facto* l'applicazione dell'aggravante speciale, prevista in caso di indebito utilizzo dell'identità digitale. Tale possibilità varia a seconda della modalità impiegata per inoculare il *software* malevolo. Può capitare, infatti, che il *botmaster* impieghi e-mail truffaldine, in cui, sostituendo la propria persona a quella di altri, inserisce allegati contenenti il *malware* ovvero dirotta la vittima, tramite indicazione di *link*, su siti malevoli: in tal caso, ben può ritenersi integrato un indebito utilizzo dell'identità altrui. Se, invece, l'infezione del dispositivo dovesse avvenire, per esempio, tramite un intervento diretto dell'*hacker* sul sistema aggredito, non troverà applicazione l'aggravante in questione. Potrà, tuttavia, venire in rilievo nel successivo impiego del dispositivo, allorquando il *botmaster* utilizzi il sistema infettato per intervenire su altri sistemi e dispositivi (specie come *proxy*[34]), in tal modo sostituendo la propria identità con quella del computer infetto con il quale opera.

2.1 - *Concorso di reati nella* net *e con la* net

Delineato il quadro delle fattispecie sussumibili nella creazione di una *botnet* occorre valutare se la permanenza dell'autore perpetui le conseguenze di un illecito già perfezionato, ma la cui consumazione perdura nel tempo, ovvero sia suscettibile d'integrare delitti autonomi, seppure tra loro omogenei. A tal proposito, non può certo negarsi che, in forza del principio di materialità, l'imputazione debba radicarsi sulla specificazione ed elencazione di singoli dati, informazioni, programmi o sistemi danneggiati, cancellati, intercettati, *etc.* Ciò nonostante, la norma incriminatrice non potrà che ritenersi integrata una sola volta, in quanto è irrilevante il numero degli oggetti immateriali su cui ricade la condotta criminosa, perfezionandosi, le relative fattispecie, alla compromissione di anche un solo elemento di quelli di volta in volta richiamati (potendo, tuttavia, il giudice apprezzarne il numero ai fini dell'art. 133 c.p.).

[34] Un *proxy* è un tipo di *server* che funge da intermediario. L'utente che intende accedere ad un *server* (una pagina web o qualsiasi altra risorsa disponibile su un altro *server*) in anonimato può accedere ad un dispositivo infetto così utilizzandolo come *server proxy*. Quest'ultimo si interpone nel normale flusso di comunicazione tra i *client* e i *server* dei servizi web, di modo che le richieste del sistema del soggetto agente arrivano prima al *server proxy* e da qui vengono rinviate al servizio richiesto, così eliminando il collegamento diretto tra il *client* e il *server* di destinazione.

Rilevano, poi, tutte le diverse fattispecie criminose, anche estranee al settore dell'informatica, che possono essere integrate mediante l'utilizzo di *botnets*. Visti i diversi usi che se ne possono fare, non a caso le *botnets* sono state infatti definite: "Swiss Army knives of the underground economy"[35].

Il disvalore complessivo della vicenda non si esaurisce nella creazione della rete, anzi: la fase di inoculazione del *malware* e di "impossessamento" da remoto dei sistemi di comando non sono altro che atti preparatori, funzionali all'esecuzione del reale progetto criminoso. Sono numerosi gli impieghi di una *botnet* riscontrati nella prassi: frodi informatiche, truffe *online*, estorsioni[36], furti d'identità, *password* e codici d'accesso, violazione di brevetti e diritti d'autore, spionaggio industriale, diffusione di materiale pedopornografico, intercettazioni, riciclaggio e, infine, atti di terrorismo[37].

Si evidenzia, inoltre, che l'impiego di una *botnet* è sempre più funzionale a garantire l'anonimato in rete e, così, ad assicurare l'impunità del soggetto criminale. Di rado, infatti, il *network* di dispositivi infetti ha una struttura gerarchica, ove al vertice è posto il *server* di *Command and Control* dal quale il fruitore della rete impartisce i comandi ai dispositivi *zombie*. Accade, di solito, che la *botnet* sia costruita secondo uno schema decentrato, in grado di sfruttare il protocollo *peer-to-peer*, grazie al quale l'autore criminoso ha la possibilità di mascherare sé stesso figurando come

[35] Cfr. C. WILSON, *CRS Report for Congress. Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,* 29 gennaio 2008, p. 5. Nel testo si cita il caso di Jeanson Ancheta, un *hacker* di 21 anni, membro del gruppo denominato "Botmaster Underground", condannato nel 2006 a 5 anni di detenzione per aver impiegato una *botnet* composta da più di 400.000 dispositivi infetti, a fronte del pagamento, da parte di diverse compagnie di marketing online, per la diffusione di un particolare programma malevolo in grado di influenzare gli acquisti degli utenti. Non solo. Il giovane *hacker* era anche solito "affittare" a terzi, dietro corrispettivo orario, la sua rete di computer infetti, per campagne di *spam*, *phishing*, di diffusione di *virus etc.* Il valore monetario per l'utilizzo di una *botnet* ai fini di attacchi informatici è oggi stimato in $ 50.000 al giorno: cfr. B. SANDYWELL, *On the globalisation of crime*, p. 52.

[36] La condotta estorsiva può essere diretta tanto agli stessi proprietari dei dispostivi infetti, facenti parte delle *botnet*, quanto a soggetti esterni alla rete, ai quali il c.d. *botmaster* indirizza tramite il proprio *network* un attacco cibernetico. Nel primo caso, ad esempio, l'utilizzatore della *botnet*, dopo essere entrato in possesso di dati del titolare del *computer zombie*, può ricattare la vittima di cancellare o diffondere tali dati informatici (immagini, documenti, dati di navigazione *etc.*) o personali. Oppure ancora, il soggetto criminale può sfruttare le potenzialità del suo strumento per inoculare, nei computer di soggetti esterni alla rete, particolari programmi malevoli, detti *ransomware*, in grado criptare i dati di un sistema informatico e renderli inservibili senza chiave di decriptazione. L'autore dell'illecito può allora offrire la chiave d'accesso in cambio di un riscatto, il più delle volte in moneta virtuale, così da evitare il tracciamento dell'operazione.

[37] Celebre l'attacco informatico perpetrato nei mesi primaverili del 2007 in Estonia, allorquando fu interrotto il funzionamento di numerosi siti web (quello del Parlamento, della Presidenza, di quasi tutti i ministeri, di banche, giornali, televisioni *etc.*) mediante un attacco *DDoS*.

uno dei nodi stessi della rete. Ne consegue, quindi, che l'utilizzo di una *botnet* può in alcuni casi prescindere da un rapporto di strumentalità con un reato-fine, per la cui realizzazione il soggetto agente ha bisogno di un mezzo pluri-strutturato (si pensi ad un attacco informatico di tipo *DDoS*), venendo in rilievo, invece, quale strumento atto a nascondere le tracce di altri reati.

La circostanza assume una rilevanza argomentativa laddove non sia possibile ravvisare la coincidenza soggettiva autore-fruitore della *botnet*, potendo darsi casi – e nella prassi sono numerosi – in cui la rete di dispositivi infetti è "affittata" a soggetti terzi, i quali impiegano il *network* per commettere reati o anche solo illecite campagne pubblicitarie. Oltre, dunque, a venire in rilievo le norme sul concorso di persone tra autore e utilizzatore della *botnet*, ci si dovrà chiedere quali siano le fattispecie attribuibili, secondo il principio di colpevolezza, al semplice fruitore e, così, se quest'ultimo debba rispondere anche della diffusione del *malware*, dell'accesso, del danneggiamento di dati e sistemi, *etc.* funzionali al funzionamento della rete.

3. *Unicità e pluralità dell'azione in ambito informatico*

Ci si chiede, a tal punto, se le fattispecie incriminatrici sinora descritte debbano trovare tutte applicazione o se l'applicazione di alcune escluda quella di altre. Prima ancora di soffermarsi sulla scelta dei criteri da adottare per risolvere il concorso di norme e di reati, occorre approfondire il tema dell'unità o pluralità dell'azione. La questione, tuttavia, non appare affatto semplice, considerato che, in materia di reati informatici, la condotta umana causativa dell'evento, in senso naturalistico e/o giuridico, si concatena necessariamente ai processi di automazione dei programmi e dei sistemi informatici impiegati[38]. Le azioni materiali, naturalisticamente intese, appaiono allora non più semplicemente riconducibili al «paradigma fisico-corporale di un movimento muscolare dell'uomo, perché immediatamente dirette ai sistemi informatici con comandi veicolati dal software»[39]. Bisogna, dunque, valutare in che modo i processi di automazione delle nuove tecnologie incidano sul piano materiale e giuridico dell'azione.

[38] Sul tema si rimanda a U. PAGALLO - M. DURANTE, *The Pros and Cons of Legal Automation and its Governance*, in *European Journal of Risk Regulation*, 2016, vol. 7, p. 323 e ss.; L. PICOTTI, *Reati informatici, riservatezza, identità digitale*, reperibile sul sito *www.aipdp.it*, p. 15 e ss.; ID., *Diritto penale e tecnologie informatiche*, p. 52 e ss.

[39] ID., *Diritto penale e tecnologie informatiche,* p. 53.

Assumiamo ancora il caso delle *botnets*. Occorre dapprima constatare l'assenza di una fattispecie incriminatrice unitaria, idonea a riprodurre sul piano giuridico, nella forma di reato complesso, abituale o permanente, l'unitarietà che, almeno concettualmente, caratterizza la creazione di una *botnet*. In quel caso, infatti, la questione avrebbe avuto minore pregnanza, in quanto l'azione, una o plurima, sarebbe stata in ogni caso riconducibile ad una sola figura delittuosa.

L'impossibilità di una unificazione giuridica, invece, conduce a ritenere decisiva la valutazione in merito all'unità o alla pluralità dell'azione, variando, in base ad essa, la natura del concorso di norme, che può essere, tanto, l'effetto di una pluralità naturalistica (ossia di una molteplicità di comportamenti, ognuno dei quali integra una violazione normativa distinta dalle altre), riconducibile alla figura del concorso *materiale*; quanto, l'effetto di una pluralità di violazioni di legge (a fronte, però, di un'unica azione materiale), in ciò distinguendosi il concorso *formale*.

Sotto questo profilo, la condotta del c.d. *botmaster*, per alcuni versi, sembrerebbe unica: una volta "diffuso" il *malware* suscettibile di provocare l'accesso e il controllo da remoto, l'alterazione, l'intercettazione, il danneggiamento dei sistemi e dei dati ivi inseriti sono tutti eventi riconducibili non più all'azione materiale del soggetto, quanto piuttosto all'esecuzione del codice malevolo da parte del sistema informatico infetto. I procedimenti di automazione dei sistemi informatici, infatti, esonerano dal compimento di ulteriori azioni il soggetto agente, la cui condotta si sostanzia nell'avviare una sequenza di elaborazione e lavorazione dei dati ad opera del programma utilizzato[40]. La condotta dell'autore criminale perde però il connotato di

[40] Si rimanda sul punto a W. VAN DER WAGEN - W. PIETERS, *From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks*, in *British journal of criminology*, 2015, vol. 55, n. 2, p. 4 e ss. Gli Autori, dopo aver identificato le diverse fasi di ideazione, creazione, utilizzo e soppressione di una *botnet*, si concentrano sull'astratta fenomenologia della pratica informatica, proponendo una diversa prospettiva d'analisi. Si ritiene, infatti, non cogliere nel segno un approccio al fenomeno incentrato sull'azione umana, sulla disamina delle singole condotte poste in essere e delle finalità perseguite dal soggetto agente. Così facendo, le componenti tecnologiche retrocederebbero a semplici strumenti necessari all'autore dell'illecito per costruire la *botnet*. Secondo gli Autori, qualora si discuta di fatti criminosi a carattere robotico e automatico, non è possibile centralizzare il fenomeno attorno al comportamento umano, in quanto sono proprio le componenti tecnologiche (come il *malware* infettato) a svolgere, in maniera del tutto autonoma, l'attività illecita; talvolta anche in modo imprevedibile, sfuggendo nel modo di comportarsi e propagandarsi alle previsioni dei loro stessi programmatori. Ciò significa che gli effetti della diffusione, in termini di scala, impatto e continuazione, non possano essere esclusivamente attribuiti al fattore umano e alle decisioni del c.d. *botmaster*. Si assume, quindi, che la natura "robotica" di questa tipologia di reati trasformi la relazione uomo-tecnologia, dall'essere unidirezionale (il soggetto che impartisce gli ordini) a cooperativa, così finendo per concepire la *botnet* come un ibrido della condotta umano/tecnologica.

unitarietà se si considera che ad essere coinvolti nella *net* sono molteplici dispositivi informatici, ognuno dei quali può appartenere a persone fisiche diverse. La diffusione del *malware* da parte dell'agente criminale, quindi, non dà avvio ad una sola sequenza, ma ad una pluralità di esse, tante quante sono i sistemi infettati.

Assumiamo che il programma malevolo sia stato inoculato previo invio di una e-mail con allegato il *virus*, spedita dal soggetto agente a più destinatari. L'inserimento di più indirizzi e-mail nel corpo di un solo messaggio, pur rappresentando figuratamente tanti invii quante sono le vittime, appare riconducibile ad un'azione materiale unica, in forza di quell'approccio pre-giuridico, di tipo naturalistico e socio-valutativo[41], che valorizza la contestualità degli atti e l'unicità del fine[42]. Si è detto, infatti, che la direzione verso un fine consapevole imprime all'azione un carattere unitario, cementando i singoli atti di cui è composta l'azione in un unico insieme. Atti che, dal canto loro, debbono susseguirsi immediatamente, senza notevole interruzione, sì da formare un indistinto complesso[43]; complesso che, nel caso di specie, può certamente riconoscersi.

Non è altrettanto chiaro se l'unicità dell'azione materiale si riproduca anche sul piano giuridico e se il reato di "diffusione" che essa integra debba parimenti ritenersi una fattispecie unitaria. Se così fosse, la diffusione sarebbe punibile una sola volta, e

[41] Cfr. F. PALAZZO, *Corso di diritto penale. Parte generale,* Giappichelli, 2016, 6ª ed., p. 219.

[42] Tale secondo elemento, a parere di alcuni autori, non sarebbe in alcun modo necessario. L'unicità del fine, infatti, non atterrebbe alla materialità dell'azione, sulla quale deve essere riguardato il comportamento umano per apprezzarne l'unità o pluralità. L'introduzione di un criterio soggettivo affianco a quello oggettivo non sarebbe motivata da alcuna pratica utilità e potrebbe avere effetti controproducenti nei casi in cui si faccia menzione di fattispecie colpose, rispetto alle quali manca in radice una prospettiva mentale coincidente con il proposito criminoso (per cui plurimi accadimenti non sarebbero mai suscettibili di unificazione).

[43] In giurisprudenza, si legga a titolo esemplificativo Cass. pen., SS.UU., 22 febbraio 2018, n. 40981: «Nel concetto di azione unica vanno ricompresi tanto i casi in cui l'azione si risolva in un "atto unico" (conforme alla condotta normativamente prevista), quanto i casi in cui l'azione si realizzi attraverso il compimento di una "pluralità di atti" che siano contestuali nello spazio e nel tempo ed abbiano fine unico. Con la precisazione che, a scanso di ambiguità, l'apprezzamento di tali caratteri (contestualità degli atti e unicità del fine) deve essere effettuato attraverso un raffronto rigoroso e costante della fattispecie astratta descritta dalla norma». Alcuni autori ritengono debba darsi rilevanza anche alla direzione degli atti all'offesa di un medesimo interesse giuridico: cfr. F. MANTOVANI, *Diritto penale. Parte generale*, Cedam - Wolters Kluwer, 2017, 10ª ed., p. 125. Tale soluzione, però, potrebbe essere fuorviante e portare, in concreto, a conseguenze irrazionali. Si pensi al caso in cui Tizio abbia colpito mortalmente Caio con un coltello al torace. Se si apprezzasse esageratamente l'interesse protetto dalla norma e offeso dal movimento corporeo, si potrebbe arrivare a considerare come azione plurima il fatto di aver trapassato il vestito di Caio (il reato di danneggiamento tutela un interesse patrimoniale) e quello di aver colpito il suo corpo (di cui il bene giuridico da tutelare è la vita umana).

ciò a prescindere dal numero dei soggetti coinvolti, finanche in presenza di più atti (ad es. più invii), tutti unificati dall'unicità del fine e dalla contestualità temporale (al pari di un unico furto in cui sono sottratti più beni nel medesimo "colpo"). Se, al contrario, a fronte della pluralità soggettiva debba inevitabilmente corrispondere una molteplicità di violazioni normative[44], l'invio di una sola e-mail determinerà l'integrazione di più reati in concorso formale.

Qualora la fattispecie prevista dall'art. 615-*quinquies* c.p. non dovesse ritenersi unitaria, il soggetto agente che diffonde il *malware* necessario alla creazione di una *botnet*, mediante più azioni materiali (si pensi a più invii di e-mail; più soggetti che accedono, in tempi diversi, sul dominio *web* infetto, *etc.*), darebbe avvio ad una pluralità di sequenze con più azioni materiali. La conseguenza, allora, sarebbe che ai successivi reati di alterazione, danneggiamento, intercettazione e accesso abusivo (per ogni sistema informatico parte della *botnet*) si applicherebbe il diverso regime del concorso materiale, salva poi la possibile unificazione normativa *quoad poenam*, riconoscendo nella creazione della *botnet* il presupposto per la continuazione, ossia l'unicità del disegno criminoso.

4. Convergenza normativa, concorso apparente e reale di reati in materia di *Botnets*

Una volta assunto che la diffusione di un *malware* o *virus*, suscettibile di provocare il controllo da remoto di dispositivi, rappresenti l'azione principale del soggetto agente (seppure a livello normativo la relativa fattispecie è considerata, per il trattamento sanzionatorio che le si riserva, di minore gravità), dalla quale poi

[44] Argomentando diversamente, si potrebbe sostenere che, solo in caso di offesa a beni altamente personali, l'azione che ricade su più soggetti provoca necessariamente una pluralità di violazioni normative (in tal senso: G. FIANDACA - E. MUSCO*, Diritto penale. Parte generale*, Zanichelli, 2001, 4ª ed., p. 615; F. PALAZZO, *Corso di diritto penale*, p. 220). Così, ove l'azione coinvolge beni di altra natura (ad esempio la sfera patrimoniale) ben potrebbe ritenersi unica, seppure fonte di danno per più persone (comunque tutte legittimate ad agire per il ristoro dei danni). Tale tesi, tuttavia, trova costante smentita dalla giurisprudenza. Cfr. *ex multis* SS.UU. n. 40981/2018: «Non sembra avere sicuro fondamento, invece, l'opinione con la quale, distinguendo tra norme incriminatrici che tutelano beni altamente personali (vita, integrità fisica, libertà personale, onore) e norme che proteggono beni di natura diversa, si afferma che nel primo caso sarebbe sempre configurabile una pluralità di reati in ragione della rilevanza dei plurimi interessi lesi, mentre nel secondo ciò non sarebbe sempre possibile. La tesi pone infatti un alone di incertezza nel giudizio di concretizzazione della fattispecie tipica, mentre sul piano normativo non paiono rinvenirsi argomenti per una distinzione di tale fatta, né criteri discretivi oggettivi che consentano di distinguere con sufficiente precisione tra i beni altamente personali e quelli che tali non sarebbero».

conseguono gli eventi di alterazione, danneggiamento, intercettazione, occorre valutare quali delle norme incriminatrici sopra riportate, tutte convergenti sul tale fatto, debbano trovare reale applicazione.

Ove si continuasse a predicare che il concorso di reati debba essere regolato mediante il criterio di specialità, unico parametro legale in base al quale risolvere l'alternativa apparenza/realtà del concorso, il principio del *ne bis in idem*, nella normativa di questo settore, avrebbe una portata assai limitata. Infatti, raffrontando le norme sul piano formale e astratto delle loro formulazioni e dei loro elementi strutturali, come stabilisce l'art. 15 c.p.[45], i reati elencati[46] (gli artt. 615-*ter*, 615-*quinquies*, 635-*bis*, 635-*quater*, 617-*quater*, 617-*quinquies*, 640-*quater* c.p.), finiscono di fatto per concorrere tra loro, salve alcune eccezioni.

L'applicazione dell'art. 635-*bis* c.p., per esempio, è certamente esclusa da quella dell'art. 635-*quater* c.p.: il reato previsto dalla prima norma, in forza del richiamo contenuto nel 635-*quater*[47], costituisce (eventualmente) un elemento di quest'ultima

[45] Tale norma non può che demandare ad una valutazione strettamente normativa, da esplicarsi sul piano puramente astratto delle relazioni logico-formali delle fattispecie. Del resto, anche da un punto di vista letterale, considerato che la norma utilizza il predicato "regolare", mal si concilierebbe la traduzione del concetto "stessa materia" con "medesima situazione di fatto concretamente verificatasi", oppure "medesimo bene giuridico". Riferendosi, dunque, ad un rapporto tra fattispecie astratte, l'indagine sull'identità della materia «viene a compenetrarsi, quindi, con l'ambito logico-strutturale entro il quale i singoli elementi delle fattispecie possono dirsi "gli stessi" o "diversi"» (così: G. DE FRANCESCO, *Lex specialis. Specialità ed interferenza nel concorso di norme penali*, Giuffrè, 1980, p. 55). Diviene pertanto necessario scomporre le singole norme che convergono sul fatto (e apparentemente applicabili) nei singoli elementi che le compongono, raffrontare le fattispecie in base al numero e al tipo di questi, onde valutare la loro identità o diversità. Si rimanda sempre a G. DE FRANCESCO, *Lex specialis*, p. 64-65; ID., voce "Concorso apparente di norme", in *Dig. disc. Pen.*, UTET, II, 4ª ed., 1988, p. 423-424).

[46] Si è scelto di non esaminare l'aggressione a sistemi informatici o telematici di pubblica utilità. Ragioni di continenza espositiva hanno suggerito all'Autore di non analizzare il concorso tra le fattispecie astratte che ne sarebbero state coinvolte, cercando così di attestare il discorso ad un livello meno complesso. Per una disamina di tali fattispecie si rimanda a: L. DE MATTEIS, *sub art.635-quinquies,* in G. LATTANZI - E. LUPO (a cura di), *Codice penale. Rassegna di giurisprudenza e di dottrina,* XII, Giuffrè, 2010, p. 243 e ss.; L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, in *Dir. pen. e proc.*, 2008, n. 6, p. 714 e ss.; I. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. e proc. pen.*, 2012, n. 1, p. 220 e ss.

[47] In realtà, come già osservato, l'art. 635-*bis* c.p. non descrive alcuna condotta, ma incrimina piuttosto la produzione di eventi. Perché l'agente sia punito, infatti, occorre verificare sul piano naturalistico l'effettiva distruzione, deterioramento, cancellazione, alterazione e soppressione di informazioni, dati e programmi informatici. Cfr. I. SALVADORI, *Danneggiamenti informatici*, in C. PARODI - V. SELLAROLI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Giuffrè, 2020, p. 608. Cfr. anche L. PICOTTI, *La ratifica della Convenzione Cybercrime*, p. 713, il quale

fattispecie, potendosi dunque intravedere tra le due norme incriminatrici un rapporto di continenza della prima nella seconda, riconducibile alla figura del reato complesso *ex* art. 84 c.p. Il 635-*bis*, in ogni caso, non sarebbe punibile a causa della clausola di sussidiarietà ivi prevista.

Sia il 635-*bis* che il 635-*quater* c.p. possono poi essere compresi nella fattispecie aggravata di "accesso abusivo" prevista dall'art. 615-*ter*, commi 2 e 3, c.p. Tale fattispecie equipara, senza darne una gradazione sanzionatoria, il danneggiamento dei sistemi informatici al meno grave danneggiamento di informazioni, dati e programmi informatici, prevedendo il prodursi di tali eventi quale elemento aggravante del reato base. Ci si chiede, allora, se l'applicazione dell'art. 615-*ter*, comma 3, c.p. escluda l'applicazione in concorso delle fattispecie di danneggiamento. In base ad una prima ricostruzione, la fattispecie delineata dall'art. 615-*ter*, comma 2, n. 3), c.p. sarebbe un reato complesso e non una fattispecie aggravata; a carattere plurioffensivo, ma con prevalenza del disvalore rappresentato dalla violazione del domicilio informatico rispetto a quello patrimoniale, come anche dimostrato dalla collocazione sistematica della norma. In tal caso, trovando applicazione l'istituto di cui all'art. 84 c.p., non si darebbe luogo a concorso formale di reati in quanto le ipotesi di danneggiamento sarebbero interamente assorbite e, così, escluse dall'applicazione in forma aggravata del 615-*ter* c.p.

È prevalente, tuttavia, una diversa interpretazione, che ravvisa nelle due norme incriminatrici un rapporto di semplice interferenza, ritenendo possibile il concorso formale tra i due reati. Il danneggiamento di sistemi o dati informatici, ai sensi dell'art. 615-*ter* c.p., rileverebbe come conseguenza anche non voluta da parte del soggetto agente[48], sicché, nel caso in cui l'autore dell'illecito abbia intenzionalmente provocato un danneggiamento, troverebbero applicazione le fattispecie incriminatrici appositamente previste dal legislatore. Quindi, a differenziare le due norme sarebbe l'elemento soggettivo, potendo ravvisarsi nel dolo, previsto dalle ipotesi di danneggiamento, l'elemento aggiuntivo specializzante le fattispecie di cui all'art. 635-

evidenzia come, nell'ambito dei reati informatici, sia effettivamente difficile distinguere i concetti di condotta ed evento.

[48] Cfr. D. FONDAROLI, *La tutela penale dei «beni informatici»*, p. 314; F. MANTOVANI, *Diritto penale. Parte speciale. Vol. 1: Delitti contro la persona*, 2019, 7ª ed., p. 622 e ss.; C. PECORELLA, *Commento all'art. 615-ter*, in E. DOLCINI - G. MARINUCCI (a cura di), *Codice penale commentato*, 2ª ed., 2006, p. 4330 e ss.; I. SALVADORI, *I reati contro la riservatezza informatica*, in A. CADOPPI - S. CANESTRARI - A. MANNA - M. PAPA, *Cybercrime*, p. 688.

bis e *quater* c.p. rispetto all'art. 615-*ter*, comma 2, n. 3), c.p., il quale – dal canto suo – potrebbe essere applicato in concorso solo nella forma base[49].

Bisogna considerare, ancora, che il danneggiamento di programmi o sistemi informatici o telematici rileva nell'art. 615-*ter*, comma 2, c.p. anche ai sensi del n. 2). Secondo la previsione, l'accesso abusivo ad un sistema informatico è aggravato «se il colpevole per commettere il fatto usa violenza sulle cose». Come indicato all'art. 392 c.p., agli effetti della legge penale «si ha altresì "violenza sulle cose" allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico». Le condotte descritte da tale norma non riproducono esattamente quelle descritte agli artt. 635-*bis* e 635-*quater*. Rispetto alla prima fattispecie, da una parte, le condotte vengono riferite solamente ai programmi informatici (e non anche alle informazioni e ai dati informatici)[50], dall'altra, viene a delinearsi un cerchio di comportamenti penalmente rilevanti che solo a livello sintattico è più ristretto, in quanto, escludendo la distruzione, il deterioramento e la soppressione, ma aggiungendovi la semplice "modifica" di programmi informatici, si anticipa in modo rilevante la tutela del patrimonio informatico. Rispetto, invece, al reato di cui all'art. 635-*quater* c.p., solo nel caso in cui la condotta del soggetto agente incida sul "funzionamento" del sistema informatico o telematico vi sarebbe sovrapponibilità della fattispecie. Ebbene, considerato che ai sensi del 615-*ter* c.p., in combinato disposto con l'art. 392 c.p., rileva l'"impedimento" o il semplice "turbamento" del sistema informatico o telematico, anche in tale caso risulta anticipata la soglia di punibilità, rispetto all'"ostacolare gravemente" di cui all'art. 635-*quater* c.p.

L'inoculazione di un programma malevolo nel dispositivo della vittima, allora, dà vita ad un concorso apparente tra la fattispecie aggravata di cui all'art. 615-*ter* e le

[49] Cfr. I. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici*, p. 234. In senso conforme anche la giurisprudenza prevalente. Così, a titolo esemplificativo, Cass. pen., sez. V, 25 marzo 2019, (ud. 25/03/2019, dep. 02/05/2019), n. 18284: «Deve essere pertanto affermato il principio per cui, in ipotesi di accesso abusivo ad una casella di posta elettronica protetta da *password*, il reato di cui all'art. 615-*ter* c.p., concorre […] con il reato di danneggiamento di dati informatici, di cui all'art. 635-*bis* c.p. e ss., nel caso in cui, all'abusiva modificazione delle credenziali d'accesso, consegue l'inutilizzabilità della casella di posta da parte del titolare».

[50] Cfr. I. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici*, p. 234 e C. PECORELLA, *Il diritto penale dell'informatica*, p. 233, i quali evidenziano un'evidente disparità di trattamento tra le ipotesi di aggressione "strumentali" di cui all'art. 392, c. 2, c.p. e quelle di violenza a danno dei singoli dati o informazioni informatiche. Si sottolinea, infatti, che solamente le prime potranno essere assorbite nell'ipotesi aggravata dell'art. 615-*ter*, comma 2, n. 2, c.p., mentre le seconde daranno luogo a concorso di reati.

ipotesi di danneggiamento di cui agli artt. 635-*bis* c.p. A differenza dell'aggravante di cui al n. 3), ove gli eventi descritti sono qualificati come conseguenza anche non voluta della condotta base, la fattispecie tipizzata al n. 2) presuppone la tenuta volontaria e, quindi, dolosa. L'elemento differenziale che prima consentiva di escludere l'apparenza del concorso con le fattispecie del Titolo XIII viene ora meno, dovendosi pertanto concludere per l'applicazione del solo art. 615-*ter* c.p., nella forma aggravata, e non anche del 635-*bis* c.p. ove la condotta violenta del soggetto coinvolga programmi informatici (non così nel caso in cui l'azione materiale ricada su dati e informazioni, rispetto ai quali ci si chiede se sia possibile risolvere il concorso in forza della clausola di sussidiarietà con la quale si apre l'art. 635-*bis* c.p.).

Quanto alla fattispecie di cui all'art. 635-*quater* c.p., assumere che il "grave ostacolo al funzionamento" si verifichi prima dell'introduzione abusiva nel sistema informatico altrui può essere difficilmente ipotizzabile. Diversamente, è ben immaginabile che il malfunzionamento sia prodromico al mantenimento del soggetto nel sistema informatico. Non è infrequente, infatti, che una volta installato il *malware* (ad esempio un c.d. *Rootkit*, realizzato per ottenere l'accesso ad un dispositivo), esso si avvalga dei permessi di Amministratore, modificando dei *software* installati nel sistema, compresi quelli nati per rilevarli e bloccarli (gli *antivirus*), così da ostacolare in modo grave il funzionamento difensivo del sistema informatico.

In tale evenienza, dunque, confrontando le due fattispecie, sembra potersi delineare un rapporto di interferenza o, come sostengono alcuni, di specialità bilaterale, insuscettibile di escludere il concorso formale di reati, in quanto attorno all'elemento comune dell'alterazione del funzionamento del sistema ruotano elementi differenti: da una parte, il mantenersi all'interno del sistema, grazie al controllo da remoto, nel 615-*ter* c.p.; dall'altra, nel 635-*quater* c.p., la previa trasmissione di un programma informatico.

Alle fattispecie descritte si aggiunge, in concorso, il reato di cui all'art. 615-*quinquies* c.p., una figura delittuosa qualificata come un antecedente logico delle norme incriminatrici indicate, ma la cui applicazione può essere esclusa solo nel caso in cui il fatto sia sussumibile anche nella fattispecie di cui all'art. 635-*quater* c.p.[51].

[51] Il criterio di specialità, lo si ricorda, unico esperibile per discernere l'apparenza/realtà del concorso, non consente di ritenere assorbita la diffusione di cui all'art. 615-*quinquies* c.p. nel più grave reato di accesso abusivo, non essendovi coincidenza di condotta, finalità e, neppure, d'azione materiale. La giurisprudenza, a tal proposito, non ha mancato di applicare le due norme in concorso: cfr. Tribunale di Bologna, sez. I, 22 dicembre 2005, n. 1823 in *Giur. mer.*, 2006, n. 5, p. 1227 e ss., con nota di C. RABAZZI, *Il reato di diffusione di virus informatici nella dottrina e nella giurisprudenza nazionale*. La

La persistente inter-connettività dei sistemi informatici tramite rete Ethernet e/o altri canali può assumere spessore autonomo sul piano delle qualificazioni giuridiche ai sensi degli artt. 617-*quater* e *quinquies* c.p. Numerose tipologie di *malware*, infatti, provocando l'accesso ai programmi informatici e telematici presenti sul dispositivo della vittima, consentono all'autore criminale di intercettare, impedire o interrompere discrezionalmente le comunicazioni che, tramite gli applicativi installati sul dispositivo infetto, intercorrono tra più soggetti (basti pensare alla possibilità di accedere da remoto alla casella di posta elettronica del soggetto passivo). Non solo. Si ritiene che le condotte descritte dagli artt. 617-*quater* e *quinquies* c.p. possano anche ricadere su una comunicazione informatica, intendendo per essa il semplice trasferimento di dati e informazioni da un sistema all'altro. Diverse tipologie di *malware*, infatti, consentono al *cyber* criminale attacchi informatici di tipo *man-in-the-middle*, ossia l'intercettazione del traffico *Internet* nelle richieste *client-server,* mediante frapposizione dell'autore nel flusso di dati, così consentendo la sottrazione o l'alterazione delle informazioni trasmesse, il dirottamento delle comunicazioni su altri canali e il reindirizzamento del traffico di navigazione verso diversi siti *web*.

Il riconosciuto concorso formale tra i reati di cui agli artt. 617-*quater* e 617-*quinquies* c.p.[52] aggiunge altri due reati all'elenco delle possibili fattispecie applicabili, senza possibilità di risolvere, mediante il criterio della specialità, la convergenza normativa in termini di mera apparenza[53]. Le fattispecie, infatti, tipizzano elementi del tutto diversi, e mentre i reati di accesso e danneggiamento attengono ad un momento statico del funzionamento dei sistemi informatici, il reato di cui all'art. 617-

stessa dottrina segnala la differenza di beni giuridici tutelati dalle norme: cfr. F. MUCCIARELLI, *Commento all'art. 4 della legge 547 del 1993*, in *Leg. pen.*, 1996, p. 58, il quale evidenzia l'indubbia collocazione sistematica della fattispecie, la cui *ratio* è da ravvisarsi nella tutela del patrimonio informatico, dell'integrità dei dati e dei sistemi, piuttosto che del domicilio informatico. In senso conforme: G. PICA, *Diritto penale delle tecnologie informatiche*, UTET, 1999, p. 98; M. CANNATA, *I delitti contro la riservatezza informatica e telematica del domicilio*, in A. CADOPPI - S. CANESTRARI - A. MANNA - M. PAPA, *I reati contro la persona. Trattato di diritto penale*, UTET, 2006, p. 560.

[52]Le due fattispecie, infatti, contemplano condotte diverse: istallazione e intercettazione. La prima è punibile a prescindere dall'effettiva intercettazione delle comunicazioni, sicché, ove l'evento sia concretamente realizzato, esso assume autonomo disvalore. Cfr. P. DUBOLINO - P. VIGNA, voce "Segreto (reati in materia di)", in *Enc. Giu.*, XLI, 1989, p. 1080; G. D'AIUTO - L. LEVITA, *I reati informatici*, p. 32.

[53] Così anche L. SCOPINARO, *Internet e reati contro il patrimonio*, p. 217, secondo la quale la procurata inservibilità totale del sistema operativo connesso ad *Internet* (oggi rilevante a sensi dell'art. 635-*quater* c.p.), provocando l'interruzione dei flussi di dati che vengono trasmessi dal sistema infetto ad altri, sarebbe sussumibile, in concorso, nella cornice dell'art. 617-*quater* c.p.

quater si riferisce al momento dinamico della trasmissione dei dati e delle comunicazioni[54].

Rileva, in aggiunta, il reato di cui all'art. 640-*ter* c.p., che, tipizzando la percezione di un profitto con altrui danno quale elemento specializzante non ricompreso in altre norme[55], si pone in rapporto di semplice interferenza (e quindi sottratto all'applicazione del criterio di specialità) con le altre ipotesi delittuose descritte.

L'elenco dei reati ascrivibili, poi, si arricchisce, quasi all'infinito, di tutte le ipotesi delittuose integrate nell'utilizzo da remoto dei dispositivi delle vittime, nonché degli eventi penalmente rilevanti (estorsione, riciclaggio, atti di terrorismo) per la cui realizzazione è stata impiegata la *botnet*. Rispetto ad essi, infatti, non è dato individuare rapporti di interferenza normativa, presupponendo, essa, la convergenza di più norme su un medesimo fatto. La molteplicità dei comandi impressi alle macchine dal *botmaster* e la realizzazione degli scopi in un momento succedaneo, pertanto, escludono l'*idem factum* presupposto dell'art. 15 c.p. A tale norma, infatti, sono estranei quei rapporti di conseguenzialità, presupposizione, continenza, che rilevano piuttosto sul piano del concreto avvicendamento di fatti, tutti riconducibili a contesti criminosi unitari.

5. Per un diverso attributo al principio del *ne bis in idem*

Per risolvere il concorso di norme nell'ambito della creazione e dell'utilizzo di una *botnet* è evidente che non ci si possa fermare a comparare fra loro le diverse

[54] Cfr. in questo senso A. MANNA - R. FLORIO, *Riservatezza e diritto alla privacy: in particolare la responsabilità per omissionem dell'internet provider*, in A. CADOPPI - S. CANESTRARI - A. MANNA - M. PAPA, *Cybercrime*, p. 930.

[55] Dottrina e giurisprudenza maggioritarie sostengono che il reato di frode informatica e quello previsto dall'art. 615-*ter* c.p. danno luogo a concorso formale, trattandosi di figure criminose che hanno presupposti giuridici diversi. Divergono, infatti, i beni giuridici tutelati, nonché le condotte sanzionate. Cfr. C. PARODI, *I reati patrimoniali*, in V. SELLAROLI - C. PARODI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, p. 108; A. MASI, *Frodi informatiche e attività bancarie*, in *Riv. pen. economia*, 1995, p. 431; G. PICA, *Diritto penale delle tecnologie informatiche*, p. 159; nonché in giurisprudenza: Cass. pen., sez. II, 6 marzo 2013, n. 13475. Si ritiene, invece, che il delitto di frode informatica assorba i danneggiamenti informatici in forza della clausola di sussidiarietà in essi contenuta (così: A. MASI, *Frodi informatiche*, p. 430). Infine, non è possibile escludere il concorso di reati con le fattispecie descritte dagli artt. 617-*quater* e ss., stante sempre la diversità dei beni giuridici tutelati e delle condotte sanzionate. Così: Cass. pen., sez. V, 9 ottobre 2020, n. 869 e, in dottrina, R. BORRUSO - G. BUONOMO - C. CORASANITI - G. D'AIETTI, *Profili penali dell'informatica*, Giuffrè, 1994, p. 120.

fattispecie legali, sull'assunto che il principio del *ne bis in idem* sostanziale si identifichi, solo, nel divieto di molteplice qualificazione normativa dello stesso fatto. In tale ambito, infatti, la convergenza normativa è l'inevitabile conseguenza della modalità di tipizzazione normativa adottata dal legislatore, il quale – piuttosto che cristallizzare specifiche tecnologie o prassi criminose – ha preferito selezionare singolarmente determinate condotte, eventi e finalità penalmente rilevanti. Non è possibile, il più delle volte, rintracciare, in astratto, rapporti di genere a specie tra le norme in concorso proprio perché, in tale ambito, si è optato per una parcellizzazione degli elementi di rilevanza penale.

Occorre, invero, un diverso apprezzamento sulla corrispondenza tra il disvalore complessivo della vicenda storica e il significato antigiuridico espresso dall'insieme delle norme incriminatrici applicabili, al fine di escludere che l'utilizzo di qualificazioni giuridiche multiple – formalmente corretto, perché le norme concorrenti sul medesimo fatto non sono in rapporto di genere a specie o perché manca l'unità dell'azione[56] – degeneri in evidente superfetazione, così producendo un'indebita sproporzione sanzionatoria[57].

Il diritto penale dell'informatica postula, dunque, una diversa applicazione del *ne bis in idem* sostanziale. Richiede, in sostanza, di interpretare il principio non tanto come divieto di molteplice qualificazione normativa dello stesso fatto, quanto piuttosto come divieto di reiterazione del medesimo giudizio di illiceità, riferito ad un quadro di vita unitario.

Soccorrono, a tal fine, quei criteri di «natura sostanziale»[58] (sussidiarietà, assorbimento, consunzione) che importano una valutazione contenutistica della norma, mediante il riferimento al disvalore oggettivo e soggettivo[59] del fatto previsto

[56] Cfr. G. BETTIOL, *Diritto penale. Parte generale*, Cedam, 1982, 11ª ed., p. 633 il quale ben evidenzia che quando si discute di concorso apparente, ai fini dell'art. 15 c.p., si presuppone l'esistenza di un medesimo fatto, storicamente inteso, di cui sia incerta la qualificazione giuridica.

[57] In ciò dando risposta a quell'interrogativo posto in M. PAPA, *Le qualificazioni giuridiche multiple nel diritto penale*, Giappichelli, 1997, p. 19: con l'espressione divieto di *bis in idem* in ambito sostanziale non è chiaro se si voglia «impedire la reiterazione del solo giudizio di rilevanza penale, ovvero [se] il divieto riguarda la molteplicità delle sanzioni». La scelta, infatti, dipenderebbe dal significato che si attribuisce al termine *idem*, nell'alternativa *factum* o *crimen* proposta dai due orientamenti, monista e pluralista, dai quali discende una diversa portata assiologica del principio, ravvisabile nella duplice possibilità di divieto di molteplice valutazione penalistica dello stesso fatto (teoria monista); oppure nel divieto di reiterazione del medesimo giudizio di illiceità (teoria pluraliste). *Ivi*, p. 42 e 61.

[58] F. PALAZZO, *Corso di diritto penale*, p. 548.

[59] Cfr. Cfr. M. ROMANO, *Commentario sistematico del codice penale. Art. 1-84,* I, 3ª ed., Milano, 2004, p. 186.

da ogni fattispecie. Il concorso di reati verrebbe, pertanto, risolto nei termini dell'*id quod plerumque accidit*: abbinando tra loro accadimenti diversi, ma riferibili ad una medesima vicenda, si potrebbe determinare un'unità di disvalore oggettivo e soggettivo[60], ritenendo il significato antigiuridico del fatto interamente esaurito dal contenuto di una sola norma (detta *consumens*) e lo scopo di entrambe realizzato, così da evitare un'indebita duplicazione sanzionatoria e una sproporzione tra fatto illecito e pena.

Grazie a questo secondo apprezzamento anche in materia di reati informatici, nella creazione e utilizzo di *botnets*, è possibile tentare di riprodurre sul piano giuridico quell'«unitarietà del quadro di vita»[61] che contraddistingue il fenomeno, così evitando di attribuire più volte, ad uno stesso autore, un fatto che esprima una gravità unitaria sul piano normativo-sociale[62].

Non può certamente tacersi l'orientamento, sino a poco tempo fa granitico, della giurisprudenza, orientato a escludere l'operatività dei criteri di consunzione e assorbimento, evidenziando il rischio di uno sviamento del giudizio penale dai canoni del principio di legalità[63]. In merito all'assenza di una base legale dei criteri di valore,

[60] *Ibidem*.

[61] A. PAGLIARO, *Concorso apparente di norme incriminatrici*, in *Riv. it. dir. e proc. pen.*, 2013, n. 3, p. 1393.

[62] Il principio del *ne bis in idem* sostanziale, infatti, risponde alla necessità «avvertita da un moderno ordinamento democratico, di non addebitare all'imputato più volte lo stesso fatto storico, purché esso *sia il momento di emersione di una unica contrapposizione cosciente e consapevole (ergo: colpevole) dell'individuo alle regole che disciplinano la vita dei consociati*». Cass. pen, Sez. IV, 29 maggio 2018, n. 26857 (corsivi nostri).

[63] Si veda, a titolo esemplificativo: «I criteri di assorbimento e di consunzione sono privi di fondamento normativo, perché l'inciso finale dell'art. 15 cod. pen. allude evidentemente alle clausole di riserva previste dalle singole norme incriminatrici, che, in deroga al principio di specialità, prevedono, sì, talora l'applicazione della norma generale, anziché di quella speciale, considerata sussidiaria»; inoltre, «i giudizi di valore che i criteri di assorbimento e di consunzione richiederebbero sono tendenzialmente in contrasto con il principio di legalità, in particolare con il principio di determinatezza e tassatività, perché fanno dipendere da incontrollabili valutazioni intuitive del giudice l'applicazione di una norma penale»: infatti, «un'incertezza incompatibile con il principio di legalità deriva anche dalla mancanza di criteri sicuri per stabilire quali e quante fra più fattispecie, pur ben determinate, siano applicabili» (così: Cass. Pen., SS.UU., 20 dicembre 2005, n. 47164). Preme in ogni caso valorizzare la considerazione, diffusa in dottrina, per la quale la determinatezza e la prevedibilità delle conseguenze giuridiche, in quanto principi di natura liberale, non potrebbero essere invocate a sostegno di interpretazioni restrittive e sfavorevoli all'imputato. Di conseguenza, vista l'alternativa tra interpretazione certa ma sempre sfavorevole (teoria monista) e interpretazione incerta ma possibilmente favorevole (a causa dell'applicazione dei criteri di sussidiarietà, assorbimento e consunzione), non può ritenersi violato il principio di legalità posto a tutela del cittadino, essendo scontato che quest'ultimo non potrà che giovarsi della seconda interpretazione.

c'è da dire, tuttavia, che "consunzione" e "assorbimento", in realtà, non sono figure autonome né identificano una specifica tipologia di rapporti, simile a quella di *genus ad speciem*. Esse sono «soltanto *esiti finali* (una norma "consuma" o "assorbe" un'altra, quando si applica in luogo di essa: ma quali saranno le condizioni perché ciò possa accadere?) collegati all'adozione di un criterio *già determinato per altra via*»[64]. Occorre dunque ricercare, non la "consunzione" o l'"assorbimento" in sé, che sono punto di arrivo, "esiti finali", ma la "matrice" che ne è causa. Ebbene, vuoi perché lo si consideri immanente nel nostro ordinamento[65], vuoi perché si ponga l'accento sulla cogenza della normativa sovranazionale che esplicitamente riconosce il divieto di punire due volte per lo stesso fatto (art. 14, § 7, del Patto Internazionale sui diritti civili e politici; artt. 4, Prot. VII, CEDU e 50 CDFUE), non c'è dubbio che nel principio del *ne bis in idem* possa oggi ravvisarvi la base legale su cui rilevare, tra diversi fatti criminosi, nessi di continenza, conseguenzialità, presupposizione, progressione, che – assunti sul piano dei rapporti delle fattispecie incriminatrici – danno vita a consunzione o assorbimento.

Nella medesima direzione, d'altronde, si è orientata la stessa giurisprudenza di legittimità, i cui recenti approdi[66] mostrano come nel nostro ordinamento stia penetrando, in totale contrasto con orientamenti precedenti, una nuova sensibilità, propensa a dare rilevanza alla natura e alla sostanza delle cose, piuttosto che al piano logico-astratto. Sull'espresso richiamo delle Corti europee ad applicare il diritto «*in a manner which renders its rights practical and effective, not theoretical and illusory*»[67],

[64] G. DE FRANCESCO, *Ne bis in idem: evoluzione e contenuti di una garanzia, nello scenario dell'integrazione europea*, in *Legislazione penale*, 24 luglio 2015, p. 12, (corsivi originari), reperibile *online* alla URL: http://www.lalegislazionepenale.eu/ne-bis-in-idem-evoluzione-e-contenuti-di-una-garanzia-nello-scenario-dellintegrazione-europea-di-giovannangelo-de-francesco/).

[65] In dottrina diverso Autori hanno riconosciuto nel *ne bis in idem* sostanziale un principio immanente nel nostro diritto positivo, vuoi perché sarebbe desumibile da un insieme di norme (cfr. F. MANTOVANI, *Concorso e conflitto di norme del diritto penale*, Bologna, 1966, p. 430); vuoi perché possa «essere egualmente ricavato dal sistema, come risultato normativo dell'elaborazione dogmatica di *un'istanza-guida di giustizia materiale*» (M. ROMANO, *Commentario sistematico del codice penale*, p. 179 (corsivi originari)); vuoi perché sarebbe «un corollario della personalità della responsabilità penale (art. 27 cpv. Cost.) e del principio di eguaglianza dei cittadini di fronte alla legge (art. 3 Cost.) ed inoltre è inerente ai diritti inviolabili dell'uomo (art. 2 Cost.)» (A. PAGLIARO, *Principi di diritto penale. Parte generale*, 8ª ed., Milano, 2003, p. 197). Ancora, ritengono il *ne bis in idem* una semplice aspirazione di giustizia, un'indicazione orientativa: G. CONSO, *I fatti giuridici processuali penali*, Milano, 1955, p. 101; R.A. FROSALI, *Concorso di norme e concorso di reati*, Milano, 1971, p. 748; M. SINISCALCO*, Il concorso apparente di norme nell'ordinamento penale italiano*, Milano, 1961, p. 61 e 87.

[66] Sul punto, si consenta ancora un rinvio a T. PIETRELLA, *Illecito e sanzione*, p. 135 e ss.

[67] Corte EDU, *case of Sergey Zolotukhin v. Russia,* 10 febbraio 2009, §80, a cui hanno fatto eco numerosi pronunciamenti sempre della Corte Edu (si veda, ad esempio*, caso Grande Stevens and others v. Italy*), nonché della Corte di Giustizia UE, dapprima in C-617/10, *caso Åklagaren c. Hans Åkerberg*

la Cassazione ha, infatti, adottato una soluzione innovativa per impedire che il concorso di norme punitive, penali ed extra-penali, violi il principio del *ne bis in idem*, consentendo al giudice di merito di guardare direttamente al concreto disvalore di un fatto criminoso, senza risultare vincolato dalle stesse cornici edittali.

Per tale via dunque, in materia di doppio binario sanzionatorio amministrativo-penale, la Suprema Corte ha ritenuto di poter riservare «al giudice nazionale [il compito di] verificare la sussistenza o meno del requisito della proporzionalità del complessivo trattamento sanzionatorio», «rispetto al disvalore del fatto, da apprezzarsi con riferimento agli aspetti propri di entrambi gli illeciti (quello penale e quello "formalmente" amministrativo) [cosicché] qualora detta valutazione dovesse condurre a ritenere il complessivo trattamento sanzionatorio lesivo della garanzia del *ne bis in idem*, nei termini sopra diffusamente richiamati, il giudice nazionale dovrà dare applicazione diretta al principio garantito dall'art. 50 della Carta dei diritti fondamentali dell'Unione Europea, disapplicando, se necessario e, naturalmente, solo in *mítius*, le norme, che definiscono il trattamento sanzionatorio»[68].

È evidente il mutamento giurisprudenziale: al sindacato giudiziale sono aperte, anzi spalancate, le porte per comprendere il disvalore complessivo del fatto e per modulare la risposta sanzionatoria in conformità al canone di proporzionalità "concreta", così consentendo una maggiore aderenza delle fattispecie astratte alla realtà dei fatti. In merito a questo nuovo apprezzamento cui è chiamata la giurisprudenza di merito, la Cassazione ha cura di evidenziare che «non possono ritenersi insufficientemente determinati i presupposti in base ai quali il giudice deve verificare la sussistenza della proporzionalità del complessivo trattamento sanzionatorio, verifiche da effettuare alla luce di parametri commisurativi riconducibili, come si è messo in luce, nel *genus* delineato dall'art. 133 c.p.»[69].

Fransson, del 26 febbraio 2013, e più recentemente (recependo l'orientamento espresso dalla CEDU nella sentenza *A. and B.v. Norway*) in: C-524/15, *caso Luca Menci*, del 20 marzo 2018; C-537/15, *caso Garlsson Real Estate SA e altri c. Commissione Nazionale per le Società e la Borsa*, del 20 marzo 2018; cause riunite C-596/16 e C-597/16, *caso E. Di Puma e A. Zecca c. Commissione Nazionale per le Società e la Borsa*, del 20 marzo 2018.

[68] Cass. pen., Sez. V, 21 settembre 2018, n. 49869. Il medesimo *iter* argomentativo è riproposto in: Cass. pen., sez. V, 21 settembre 2018, n. 49869 (Chiarion); Cass. civ., sez. trib., 30 ottobre 2018, n. 27564; Cass. pen., sez. V, 16 luglio 2018, n. 45829 (Franconi); Cass. pen., sez. V, 9 novembre 2018, n. 5679 (Erbetta); Cass. civ., sez. II, 6 dicembre 2018, n. 31634; Cass. civ., sez. II, 6 dicembre 2018, n. 31632; Cass. pen., sez. V, 15 aprile 2019, n. 39999; Cass. civ., sez. II, 17 dicembre 2019, n. 33426.

[69] Sempre Cass. pen., Sez. V, n. 49869/2018. In modo simile Cass. pen., n. 39999/2019: « Il Collegio condivide, altresì, al fine di procedere alla valutazione sul rapporto tra afflittività globale della sanzione integrata e disvalore del fatto commesso, il richiamo ai parametri normativi previsti dall'art. 133 c.p.,

Si ritiene, allora, che questo nuovo orientamento ermeneutico possa valere anche nell'ambito che ci occupa, ossia al di fuori dei casi di doppio binario sanzionatorio. In quel settore, infatti, considerato che la stessa formulazione normativa richiede un concorso effettivo tra norma penale ed extrapenale[70], la non applicazione di una delle norme da parte del giudice comporta sempre una deroga, seppure *in bonam partem*, al principio di legalità (ancorché quel principio attenga, invero, alla salvaguardia del cittadino nei confronti della potestà punitiva statuale). Al contrario, in caso di concorso di norme penali, l'operare dei criteri di "consunzione" e "assorbimento"[71] non è escluso *littera verbis* dalle norme incriminatrici, potendo – quindi – farvi ricorso con ancor minore sacrificio (se così vogliamo ritenerlo), vale a dire senza neppure derogare al testo normativo[72].

6. Reati informatici e nuova giustizia penale

Il principio del *ne bis in idem*, interpretato non solo come duplice divieto di molteplice qualificazione giuridica dello stesso fatto, ma, in particolare, come divieto di reiterazione del medesimo giudizio di illiceità a fronte di un accadimento unitario,

utili a (ri)proporzionare la sanzione complessivamente inflitta, tenendo conto di un "allargamento" dell'oggetto di tali valutazioni, che, per un verso, devono essere estese al trattamento sanzionatorio inteso come comprensivo anche della sanzione formalmente amministrativa e, per altro verso, devono investire il fatto commesso nei diversi aspetti propri dei due illeciti (quello penale e quello "formalmente" amministrativo)».

[70] Non lascia spazio a fraintendimenti la clausola di salvaguardia «salve le sanzioni penali quando il fatto costituisce reato» prevista nelle fattispecie degli illeciti amministrativi di cui agli artt. 187-*bis* e 187-*ter* TUF, che rende inapplicabile il principio di specialità previsto all'art. 9, l. n. 689/1981.

[71] Invero la Corte di Cassazione fa esclusivo riferimento all'"assorbimento", sostenendo che: «Solo in presenza di una sanzione irrevocabile idonea, da sola, ad "assorbire" il complessivo disvalore del fatto, dunque, il giudice comune dovrà disapplicare in toto la norma che commina la sanzione non ancora irrevocabile, così escludendone l'applicazione sanzione». *Ibidem*.

[72] Cfr. ancora T. PIETRELLA, *Illecito e sanzione*, p. 162. Si potrebbe contestare a tal riguardo che l'approdo giurisprudenziale cui è giunta la Cassazione non possa trovare applicazione in altri ambiti, in quanto la diretta applicazione dell'art. 50 CDFUE sarebbe esclusa ove non sia ravvisabile la competenza dell'UE nella materia di riferimento. Tuttavia, è bene osservare che – come rilevato dalla stessa Corte di legittimità – la necessità di valutare il disvalore del fatto e di derogare *in mìtius* alla normativa penale in caso di evidente sproporzione della sanzione complessiva discende direttamente dalla garanzia del *ne bis in idem*, come sancito dalle Carte dei diritti e interpretato dalle loro Corti. Al giudice nazionale, quindi, si impone un'interpretazione conforme dello strumentario di diritto penale alla luce dell'art. 4, Prot. VII, CEDU, che pur non avendo diretta applicazione sì da consentire la disapplicazione della normativa interna, dà modo all'autorità giudiziaria di modellare l'ordinamento penale secondo i percorsi ermeneutici della giurisprudenza europea.

consente allora di rimediare a quegli eccessi di criminalizzazione che la tecnica di normazione adottata in ambito informatico rischia di generare. Rispetto ai c.d. *computer crimes*, la formulazione delle fattispecie delittuose risulta generica se la si raffronta alla specificità e tecnicismo delle tecnologie utilizzate, così rappresentando un *vulnus* alla legalità penale. La possibilità di calibrare la risposta sanzionatoria in base al complessivo disvalore del fatto, mediante il ricorso a meccanismi di "assorbimento" e "consunzione" da parte dell'autorità giudiziaria, consente diversamente di recuperare, *nel concreto*, quella tipicità legale che *sul piano delle formulazioni astratte* è invece deficitaria.

Con particolare riguardo alla creazione di una *botnet* e al suo utilizzo, rilevare e dare importanza a quei particolari nessi (di tipo causa-effetto, mezzo-fine, di accessorietà, presupposizione, *etc.*) che possono instaurarsi tra fattispecie concorrenti su una medesima vicenda significa, concretamente, espungere dall'imputazione determinate tipologie di reati, potendo ritenerle assorbite e comprese nell'applicazione di altre. Non solo. A ben vedere, si consente anche all'ordinamento di calibrare la risposta sanzionatoria in base alla specificità delle tecnologie impiegate, come la tipologia di *malware* utilizzato, le modalità di inoculazione, le capacità aggressive del *software*, riconoscendo la prevalenza ora alle fattispecie di intercettazione, ora ai danneggiamenti, ora agli accessi abusivi.

Così, ad esempio, la diffusione di programmi infetti, di cui all'art. 615-*quinquies* c.p., ben potrà essere assorbita, quale presupposto, nella condotta di accesso abusivo, danneggiamento o intercettazione. Se, poi, la rete di *bots* è realizzata al fine di commettere attacchi del tipo *DDoS*, potrà ritenersi prevalente la fattispecie di installazione di apparecchiature atte ad intercettare di cui all'art. 617-*quinquies* c.p., valorizzando il dirottamento delle connessioni *Internet* dei dispositivi infetti sul medesimo *server*, semmai in concorso con il danneggiamento (questo riferito non al dispositivo facente parte della rete infetta, ma ai dati e sistemi informatici destinatari dell'aggressione) ove l'attacco informatico sia poi effettivamente perpetrato. Non è da escludere, poi, che lo stesso danneggiamento del sistema aggredito dall'attacco informatico possa a sua volta ritenersi assorbito in un diverso reato-fine.

Ancora, avrà carattere prevalente e assorbente la "frode informatica", peraltro in forma aggravata, nel caso in cui la rete di *computer-zombie* sia utilizzata dall'agente criminale per campagne di *spamming*, mediante l'invio massivo di e-mail pubblicitarie

non desiderate per il tramite degli account delle vittime[73], così come per una c.d. *fraud-click*[74] o per l'installazione di *adware* o di *software* indesiderati, progettati al fine di far apparire messaggi pubblicitari sullo schermo del computer infettato.

Rimane un dato fondamentale: occorre prendere consapevolezza circa la «necessità di una profonda revisione di alcune fondamentali categorie dogmatiche, su cui si fonda la responsabilità penale, a partire da quelle di "azione" e di "evento" nel *Cyberspace*, alla luce dell'automazione, della dematerializzazione, dell'interazione fra utenti e con gli ISP[75], della diffusione e permanenza nel tempo e nello spazio degli effetti di ogni attività dell'uomo che vi si svolge, con importanti ricadute anche pratiche sulle regole d'imputazione oggettiva e soggettiva, sulla determinazione del momento e del luogo di consumazione ovvero di "esaurimento" del reato, sulla rilevanza penale di comportamenti anche successivi alla "formale perfezione" della fattispecie»[76].

In questo senso, la possibilità per il giudice di poter indagare il disvalore complessivo del fatto e, tramite l'utilizzo di meccanismi di assorbimento e

[73] Se guardata dal punto di vista del destinatario dell'e-mail pubblicitaria non desiderata, la pratica dello *spamming* assume un autonomo e diverso disvalore penale, venendo ad integrare la fattispecie di "trattamento illecito di dati" di cui all'art. 167 d.lgs. n. 196/2003. Si evidenzia però, a tal proposito, che non è sufficiente la ricezione di una comunicazione non desiderata: «Affinché tale condotta assuma rilievo penale, occorre che si verifichi per ciascun destinatario un effettivo "nocumento", che non può certo esaurirsi nel semplice fastidio di dover cancellare di volta in volta le mail indesiderate, ma deve tradursi in un pregiudizio concreto, anche non patrimoniale, ma comunque suscettibile di essere giuridicamente apprezzato, richiedendosi in tal senso un'adeguata verifica fattuale volta ad accertare, ad esempio, se l'utente abbia segnalato al mittente di non voler ricevere un certo tipo di messaggi e se, nonostante tale iniziativa, l'agente abbia perseverato in maniera non occasionale a inviare messaggi indesiderati, creando così un reale disagio al destinatario». Così: Cass. pen, sez. III, 20 settembre 2019, n. 41604.

[74] Con tale espressione si designano le condotte di sfruttamento illecito dei servizi di "*Pay-per-Click*", adottato dalle società di *marketing online*, come ad esempio Google AdSense. Lo schema criminoso è il seguente. Nell'ambito di campagne pubblicitarie, gli operatori economici si avvalgono (a titolo oneroso) dei servizi di inserzione *online* di annunci offerti da Google. Quest'ultima colloca i suddetti annunci pubblicitari nei siti che prendono parte al programma AdSense, corrispondendo ai proprietari di tali siti una percentuale per ogni *click* effettuato dagli utenti della rete su tali pagine. Mediante l'utilizzo di una *botnet*, il c.d. *botmaster* ha la capacità di generare una molteplicità di *click* sugli annunci esposti nelle pagine web, a sé stesso riconducibili o a terzi che a lui si siano rivolti. In tal modo, il proprietario della pagina web che ha aderito al programma di Google AdSense ha la possibilità di ricavare un illecito vantaggio, intervenendo senza diritto sui *computer-zombie* appartenenti alla rete infetta e provocando, non di meno, un nocumento alla società di *marketing* e all'operatore economico che, dal canto suo, non avrà alcun ritorno economico per il servizio attivato.

[75] Sta per *Internet Service Providers*.

[76] L. PICOTTI, *Diritto penale e tecnologie informatiche*, p. 43; ID., *Reati informatici*, p. 15.

consunzione, risolvere l'astratta convergenza normativa, consente un adattamento dell'ordinamento penale e dei suoi istituti alle peculiarità del *cyberspace*. Il principio del *ne bis in idem* sostanziale, nell'ottica richiamata, contribuisce a superare quel rigido e sterile formalismo in cui il sistema rischia di incagliarsi, specie nel tentativo di applicare le categorie tradizionali a fenomeni di natura informatica.