GIURISPRUDENZA PENALE

La rilevanza dei delitti contro l'integrità dei dati dei programmi e dei sistemi informatici al tempo della guerra russo-ucraina.

di ***Federica De Simone***

Sommario. 1. I nuovi scenari bellici della *cyberwar* e della *cyberwarfare*. – **2.** Le linee guida previste dal Manuale di *Tallin*. – **3.** Gli attacchi *Denial of service* e la questione definitoria. – **4.** L'inquadramento normativo. – **5.** La disciplina codicistica. – **6.** Le fattispecie previste dagli artt. 635 *bis*, *ter*, *quater* e *quinquies* c.p. – **7.** Il regime delle circostanze aggravanti. – **8.** Questioni in tema di concorso di norme e di reati. – **9.** Alcuni rilievi conclusivi.

La dimensione del cyberspazio ha assunto una crescente rilevanza sia nella sfera pubblica, sia in quella privata e ha apportato significativi benefici nella vita dei singoli e delle collettività. Ne sono conseguiti, tuttavia, risvolti negativi soprattutto in termini di rischi per la sicurezza degli attori statali e non statali. Gli attacchi Denial of service perpetrati a danno degli Stati durante la guerra russo-ucraina in corso ne costituiscono un recente esempio, alla stessa stregua di quelli subìti da alcune istituzioni pubbliche anche italiane in tempo di pace. È necessario, allora, analizzare il problema definitorio e, conseguentemente, le fonti normative da applicare.

***

The dimension of cyberspace has assumed a growing importance in both the public and private spheres and has brought significant benefits to the lives of individuals and communities. This has, however, led to negative consequences, especially in terms of security risks for state and non-state actors. The Denial of Service attacks perpetrated against states during the ongoing Russian-Ukrainian war are a recent example, as are those suffered by some public institutions, including Italian in peacetime. It is necessary, then, to analyze the definitional problem and, consequently, the normative sources to be applied

1. I nuovi scenari bellici della *cyberwar e della cyberwarfare*

Sin dall'inizio del conflitto che vede tutt'oggi contrapposte Russia e Ucraina è stato evidente che il fronte bellico non fosse solo quello fisico che vede coinvolti i territori in senso stretto. Altrettanto attivo e capace di offensive pesanti, infatti, è anche il fronte *cyber*, che si sviluppa in tre diverse modalità tecnico-operative.

La prima riguarda la manipolazione dell'informazione, sia in termini di propaganda sia di disinformazione, che ha spinto l'Europa e le principali piattaforme *social* a bloccare alcune trasmissioni russe[1], pur cercando di garantire alle popolazioni coinvolte le comunicazioni internet e l'informazione libera. Proprio in quest'ottica si colloca il Regolamento Ue 328/2022 del 25 febbraio 2022 dettato in tema di *Misure restrittive in considerazione di azioni della Russia che destabilizzano la situazione in Ucraina* e che fa espresso divieto di esportazione verso la Russia di molti beni che riguardano i settori dell'*Information and Communication Technology* (ICT), come materiali elettronici, telecomunicazioni e sicurezza dell'informazione[2].

La seconda modalità si sostanzia nel lancio di attacchi *Denial of service*[3] finalizzati alla distruzione, deterioramento, cancellazione, alterazione e soppressione dei sistemi informatici istituzionali e delle infrastrutture digitali dei paesi coinvolti nel conflitto. A dispetto di quanto si possa credere, un attacco informatico di questo tipo può avere una portata lesiva paragonabile a quella di un attacco militare di tipo tradizionale o, addirittura, essere anche più grave, ove determini un coinvolgimento globale. Le conseguenze, infatti, si misurano in termini di interruzioni di servizi strategici, di infrastrutture terrestri e satellitari e possono incidere in maniera significativa sulla tenuta del sistema di uno Stato. Tant'è vero ciò, che gruppi organizzati di *hacker* si

---

[1] Il 1 marzo 2022 il Consiglio dell'Unione europea ha adottato, in base all'art. 29 dei Trattati, una decisione secondo cui *è proibito* [con qualsiasi mezzo] *per gli operatori di trasmettere, od anche aiutare, facilitare ed in alcun modo contribuire alla trasmissione qualsiasi entità giuridica menzionata nell'annesso alla decisione, e cioè: Russia Today English, Russia Today UK, Russia Today Germany, Russia Today France, Russia Today Spanish & Sputnik*. […] *Sono altresì sospese tutte le licenze di trasmissione riguardanti RT e Sputnik su tutto il territorio della UE ed è severamente proibito di contribuire ad attività volte a vanificare queste disposizioni*. Il Consiglio giustifica il provvedimento, peraltro già adottato nel 2014 in occasione del conflitto nel Donbass e a seguito dell'annessione della Crimea, alla luce della considerazione che *la Federazione Russa si è impegnata in una sistematica campagna internazionale di manipolazione dei media e di distorsione dei fatti, che ha come motivazione lo scopo di mettere in pratica una strategia di destabilizzazione dei paesi vicini, oltre ché dell'Unione Europea e degli stati dell'Unione. Questa azione di propaganda è stata condotta attraverso una serie di canali o media sotto il controllo diretto o indiretto della leadership della Federazione Russa e mette a repentaglio la sicurezza e l'ordine pubblico dell'Unione*.

[2] Cfr. *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R0328&from=IT*, modificato dal Regolamento (UE) 2022/350 del Consiglio del 1 marzo 2022 e rinvenibile in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L:2022:065:FULL&from=EN*.

[3] Da ora i *Denial of Service* saranno indicati con l'acronimo *DoS*.

fronteggiano dalle linee digitali russe e ucraine alla stessa stregua di quanto fanno i contingenti militari al fronte.

Infine, nella terza procedura gli attacchi *DoS* sono rivolti nello specifico al blocco dei terminali delle organizzazioni che si occupano di logistica, rifornimenti e gestione dei fondi riguardanti la crisi umanitaria e il flusso di profughi.

Invero, tra gli scenari della guerra cibernetica è necessario operare una distinzione tra *cyberwar* e *cyberwarfare* che non è solo terminologica, individuando contesti operativi e finalità diversi, ma che tuttavia non è così netta, potendo dare luogo a una coincidenza di attività, tale da determinare il ricorrere di entrambe le ipotesi. La principale differenza risiede – stando alle definizioni maggiormente condivise in dottrina[4] – nelle finalità perseguite dalle condotte poste in essere, a parità di oggetto su cui ricadono.

Con il termine *cyberwar*, infatti, si fa riferimento a tutto il contesto bellico nel suo complesso, che presuppone una dichiarazione di guerra anche implicita e lo svolgimento di una serie di attività militari di tipo cibernetico, tra cui veri e propri atti di spionaggio. In particolare, l'agente (statale e non) conduce operazioni militari allo scopo, da un lato, di carpire informazioni sull'avversario e di impedire allo stesso di utilizzarle a suo vantaggio, dall'altro di interrompere o distruggere le informazioni stesse e i sistemi di comunicazione. Si determina, così, uno squilibrio nell'uso e nella circolazione dei dati e delle informazioni che avvantaggia l'aggressore, compromettendo la capacità dell'aggredito di operare delle scelte difensive anche sul terreno della guerra intesa in senso tradizionale.

Diversamente, nell'ipotesi della *cyberwarfare* gli atti bellici, pur avendo ugualmente ad oggetto le tecnologie dell'informazione delle comunicazioni, concretizzano una strategia militare offensiva o difensiva mirata all'interruzione immediata o al controllo delle risorse del nemico. In tale contesto gli agenti e gli obiettivi sono rinvenibili sia nel dominio fisico, sia in quello cibernetico e il livello di violenza può variare a seconda delle circostanze, con una intensità che può raggiungere livelli anche molto elevati in termini di progressivo aumento delle operazioni belliche[5].

---

[4] Sul punto si veda ARQUILLA J., RONFELDT D., *Cyberwar is coming!*, Santa Monica, CA: RAND Corporation, 1993 in *http://www.rand.org/pubs/reprints/RP223.html* e TADDEO M., *An analysis for a just cyber warfare, International Conference on Cyber Conflict* (CYCON 2012), IEEE ed., Tallin 2012, pp. 1-10.

[5] Definizione puntuale della *cyberwarfare* la descrive come *l'impiego di incisive tecniche di intrusione o sabotaggio delle risorse informatiche e fisiche di un paese avversario, effettuate in un contesto bellico, attraverso l'impiego di computer e reti di telecomunicazioni informatiche, volte a compromettere le difese, il funzionamento e la stabilità economica e sociopolitica del nemico*. Così L'INSALATA M., *Cyberwarfare: gli scenari della guerra informatica*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano 2019, pp. 1273 ss., che opera anche una distinzione tra la

Da un simile scenario emerge che gli attacchi *DoS* costituiscono la principale arma impiegata nella *cyberwar* in generale e nella *cyberwarfare* in particolare, mentre al di fuori di uno scenario di guerra eventuali attacchi sferrati da uno Stato a danno di un altro sarebbero da inquadrarsi in attività di *cybercrime* in senso lato[6].

Nel primo caso le condotte si qualificano come veri e propri atti di guerra, da cui dovrebbero discendere inevitabili conseguenze militari a seguito dell'applicazione dello *ius ad bellum* internazionale anche al *cyberspazio*. Diversamente, nel secondo caso la qualificazione di tali condotte come atti di *cybercrime* determina l'operatività della normativa nazionale che, in Italia, si traduce nell'applicazione degli articoli 635 *bis* e seguenti del codice penale, dettati in tema di *delitti contro l'integrità dei dati dei programmi e dei sistemi informatici*.

Invero, il confine tra le due ipotesi è alquanto labile. Proprio la guerra in corso tra Russia e Ucraina mostra, infatti, come gli atti militari che segnano l'inizio di un conflitto armato siano preceduti da attacchi informatici diretti a destabilizzare anzitempo il nemico, scoprirne la capacità difensiva e carpirne le strategie militari[7]. Ne consegue che in tale ipotesi le condotte tipiche del *cybercrime* sono prodromiche alla guerra cibernetica. Anche ove non lo fossero, si tratta di condotte a cui gli Stati ricorrono sempre più frequentemente per valutare l'inoppugnabilità di un paese ostile o per comprometterne la stabilità, tanto che alcuni ritengono si tratti di una vera e propria guerra in tempo di pace, in cui manca la veste ufficiale del conflitto militare e la progressiva intensificazione degli sforzi bellici[8].

Sia che si guardi solo agli attacchi informatici occorsi duranti le operazioni militari, sia che si guardi a quelli che le precedono, rimane da affrontare la questione relativa all'opzione normativa da seguire, con la consapevolezza che il carattere ibrido di questi attacchi rende difficile tracciare un confine netto[9]. Ciò posto, per i primi, in particolare, la questione immanente da

---

cyberwarfare di tipo strategico e quella di tipo operativo (p. 1279). Si veda anche ROBINSON M., JONES K., JANICKE H., *Cyber warfare: Issues and challenges*, in *Comput. & Secur.*, 2015, 49, pp. 70–94.

[6] MARRONE A., SABATINO E., CREDI O., *L'Italia e la difesa cibernetica*, in *https://www.iai.it/sites/default/files/iai2112.pdf*, p. 33, parlano di guerra cibernetica in tempo di pace, equiparandola sotto alcuni profili alla guerra fredda.

[7] Per una ricostruzione degli attacchi *DoS* da parte della Russia ai danni dell'Ucraina prima dell'avvio del conflitto si veda *https://www.cybersecurity360.it/nuove-minacce/guerra-cibernetica-gli-impatti-del-conflitto-russia-ucraina-e-il-contrattacco-di-anonymous/*.

[8] Cfr. SILVESTRI S., *Guerre nella globalizzazione: il futuro della sicurezza europea*, in IAI Papers, 2012, 20, in *https://www.iai.it/it/node/11674*.

[9] Secondo alcuni *il dominio cibernetico è considerato uno dei campi privilegiati della cosiddetta "guerra ibrida", condotta utilizzando senza soluzione di continuità tutte le*

dirimere riguarda la possibilità di qualificare un attacco *DoS* in termini di atto armato, che – in quanto tale – contrasterebbe con il principio sancito dall'art. 2 par. 4 Carta ONU[10].

Le questioni che si agitano sul punto sono svariate e non di facile soluzione, tanto che a livello internazionale le posizioni sono anche molto divergenti, a cominciare proprio dalla possibilità di ravvisare l'uso della forza nell'atto cibernetico. La difficoltà nasce non tanto in capo alle ipotesi in cui un attacco *DoS*, interrompendo un sistema informatico, determini un danno alle infrastrutture, bensì per quei casi in cui la dimensione fisica è più evanescente, come – ad esempio – quando l'attacco determina la perdita di dati o informazioni.

Ancora, ci si chiede se un simile attacco possa dare luogo a una legittima difesa ai sensi di quanto previsto dall'art. 51 della Carta ONU e se debba essere preceduto necessariamente da un attacco di tipo tradizionale. Pur non mancando, nel panorama internazionale, voci a favore della possibilità di configurare una *difesa anticipativa*, rimangono evidenti alcune difficoltà, soprattutto rispetto alla necessità che siano comunque ravvisabili dei segnali dell'imminente attacco. Le operazioni informatiche, infatti, sono per loro natura invisibili, oltre che veloci, e ciò rende difficile la prevenzione degli stessi e la prova dell'imminenza dell'attacco[11].

Proprio gli aspetti tecnico-operativi contribuiscono a rendere più difficile l'individuazione di una soluzione, posto anche l'elevato grado di sviluppo di queste tecnologie[12]. In particolare, potrebbe risultare arduo individuare l'autore dell'attacco *DoS* e, in alcuni casi, il bersaglio stesso, potendo il segnale essere inviato contemporaneamente da *server* situati in paesi diversi[13].

Resta, infine, una questione tutt'altro di poco conto e relativa al tipo di risposta difensiva che sarebbe ammissibile in proporzione, laddove una

---

leve a disposizione del potere statuale che, dall'uso delle forze speciali alla manovra militare convenzionale, ha trovato massima espressione nell'occupazione russa della Crimea nel 2014. Così MARRONE A., SABATINO E., CREDI O., *L'Italia*, cit., p. 33.

[10] La disposizione prevede che […] *i Membri devono astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza, sia contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite* […].

[11] LAHMANN H., *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution*, Cambridge, 2020.

[12] Si veda anche LELE A., *Disruptive Technologies for the Militaries and Security*, Singapore 2019, *passim*.

[13] Cfr. DINNISS H., *Cyberwarfare and the laws of war*, New York 2014, p. 4, secondo cui ciò incide anche sulla *determinabilità ex ante del risultato di un attacco cibernetico e rende ancora più incerta la incerta l'integrazione dell'uso della forza internazionale e, conseguentemente, l'applicabilità del diritto di guerra*.

qualificazione dell'attacco cibernetico in termini di atto di guerra potrebbe – a tal punto – legittimare un'offensiva militare. La questione investe soprattutto la tipologia di risposta difensiva a un attacco *DoS* e la possibilità di rispondere con un vero e proprio atto militare a un attacco cibernetico. Per quanto ci è noto, sin ora l'unico paese a operare in questo modo è stato Israele, che nel 2019 ha lanciato un attacco missilistico dopo aver subito un attacco *DoS* da parte dell'organizzazione politica e paramilitare palestinese *Hamas*[14].

2. Le linee guida previste dal *Manuale di Tallin.*

Allo stato attuale non esiste una disciplina normativa *ad hoc* da applicare ai casi di *cyberwar* e *cyberwarfare*. Ciononostante, sono stati condotti da gruppi di esperti degli studi in merito all'applicabilità del diritto internazionale, in termini di *ius ad bellum* e di *ius in bello*, ai casi di attacchi cibernetici provenienti sia da attori statali sia da attori non statali.

Una prima versione di tali linee guida è maturata nel 2013, a seguito di un progetto sviluppato in un centro di eccellenza della NATO in Estonia[15] ed è stata presentata nel *Tallinn Manual on the International Law Applicable to Cyber Warfare*[16].

In considerazione del fatto che ai lavori non avevano preso parte tutti i paesi membri, nel 2017 il documento è stato rivisitato da un gruppo più rappresentativo di ricercatori[17], che, dopo aver recepito quanto già elaborato

[14] Sul punto si veda SETTI S., *Diritto e guerra cibernetica,* in *www.sicurezzanazionale.gov.it*, p. 7. Cfr. *https://www.agendadigitale.eu/sicurezza/i-missili-in-risposta-a-un-attacco-cyber-cosi-israele-riscrive-la-cyber-war/*. La Carta ONU prevede all'art. 51 che *Nessuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale* […].

[15] La ricerca è stata condotta presso il *Cooperative Cyber Defence Centre of Excellence* di *Tallin* in Estonia, istituito dalla NATO a seguito di un grave attacco cibernetico sferrato ai danni proprio dell'Estonia nel 2007 e di quello subito dalla Giorgia nel 2008, paese notoriamente molto avanzato nello sviluppo e nell'impiego di tali tecnologie. Al Centro ha aderito anche l'Italia, inviando propri esperti e ricercatori.

[16] AAVV, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge 2013.

[17] Ai lavori per la nuova versione del Manuale hanno preso parte non solo alcuni esperti di Diritto internazionale dei vari paesi coinvolti nel progetto, ma anche alti ufficiali militari e osservatori privilegiati come la Croce Rossa, il Comando Supremo della NATO e il Comando cibernetico USA.

in precedenza, ha innovato i contenuti e provveduto a pubblicare il *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[18].
In entrambi i casi non si tratta di documenti ufficiali, cionondimeno le regole individuate ben si prestano a costituire le fondamenta della regolamentazione di queste nuove situazioni di conflitto, consentendo di verificare l'applicabilità del diritto internazionale e del diritto bellico anche ai conflitti nel *cyberspazio*[19] e delimitando, così, i margini di operatività delle normative nazionali per tutti gli altri casi in cui i *cybercrime* in particolare, e gli attacchi *DoS* nello specifico, determinano l'operatività di fattispecie *ad hoc*.
I provvedimenti assumono la veste di una raccolta di precetti commentati, in cui sono riportate le opinioni degli esperti con particolare riguardo a quelle dissenzienti; ciò che rileva particolarmente è che, in mancanza di una regolamentazione specifica, simili testi potrebbero assurgere al rango di fonte consuetudinaria, diventando così la disciplina di riferimento sul tema[20].
Le nuove regole, che nella prima edizione del Manuale erano novantacinque e a oggi sono centocinquantaquattro, evidenziano uno sforzo definitorio ulteriore dei nuovi fenomeni e il tentativo di superare il limite della mancata estensione delle norme di Diritto internazionale pubblico alle operazioni militari in tempo di pace, pur mancando ancora riferimenti al Diritto penale internazionale, al Diritto internazionale commerciale e in ultimo alla proprietà individuale[21].
La complessità del Manuale è tale da non permettere in questa sede una puntuale disamina di tutte le parti in cui si articola; giova, però, sottolineare che la prima parte è dedicata al rapporto tra il Diritto internazionale generale e il *cyberspazio*, in cui, tra i principi fondamentali, assume un ruolo di rilievo quello previsto alla Regola n. 6 e noto come *due diligence*.
Si tratta di un principio generale del Diritto internazionale, secondo cui gli Stati sono obbligati a garantire che il loro territorio non venga utilizzato per

---

[18] AAVV, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge 2017.
([19]) Cfr. LUCANIA P., *Il manuale di Tallin: diritto e cyber war*, in *https://www.cesi-italia.org/articoli/172/il-manuale-di-tallin-diritto-e-cyber-war*.
[20] Invero, ad avviso di chi scrive, la delicatezza del tema è tale da non far ritenere appropriata una simile soluzione, essendo preferibile l'adozione di una normativa in senso stretto, condivisa dagli Stati aderenti. Cfr. LIIVOJA R., MCCORMACK T., *Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello*, in GILL T., GEIß R., HEINSCH R., MCCORMACK T., PAULUSSEN C., & DORSEY J. (a cura di), *Yearbook of International Humanitarian Law*, 2012, 15 in *https://www.researchgate.net/publication/289343354_Law_in_the_Virtual_Battlespace_The_Tallin_Manual_and_the_Jus_in_Bello/references*.
[21] SCHMITT M.N. (a cura di), *Tallinn manual 2.0 on the international law applicable to cyber operations*, Cambridge 2017, in *https://doi.org/10.1017/9781316822524*.

ledere i diritti di un altro Stato e che si ritiene possa costituire uno standard di diligenza anche rispetto alle condotte poste in essere nel *cyberspazio*. Nel Manuale di *Tallin 2.0*, infatti, gli esperti affermano che, in assenza di una espressa previsione di senso contrario, anche le nuove tecnologie sono soggette alla legge preesistente. Ne consegue, dunque, che il divieto di violazione del principio di sovranità degli Stati trovi applicazione anche nel *cyberspazio* e la regola della *due diligence* si applica a tutte le operazioni informatiche, anche quelle poste in essere da terzi o da attori non statali[22]. Ciò trova una giustificazione ontologica nella considerazione che anche le attività cibernetiche possono diventare veri e propri atti di forza ove costituiscano una concreta minaccia[23].

Gli esperti hanno contezza del fatto che dal 2007[24] ad oggi la portata dannosa di simili attacchi ha subito una evoluzione ed è ben diversa dai primi fatti descritti, con la conseguenza che l'estensione del Diritto internazionale al *cyberspazio* può costituire uno dei pilastri della pace e della sicurezza mondiale. Al contempo è anche evidente come la tematica in esame sia in continua evoluzione e come questo renda necessario aggiornare le riflessioni soprattutto in riferimento alla normativa da applicare. Tant'è vero ciò, che nel 2021 Il Centro di eccellenza per la difesa informatica cooperativa della NATO (CCDCOE) ha lanciato il *Tallinn Manual 3.0 Project*, con l'intento di rivedere i temi già affrontati e individuarne di nuovi. Il progetto ha una durata quinquennale e la natura del Manuale rimarrà invariata, dal momento che continuerà a essere un lavoro accademico non giuridicamente vincolante, finalizzato a una riaffermazione obiettiva del diritto internazionale applicato nel contesto cibernetico[25].

Pur distinguendosi ancora tra gli attacchi *DoS* in tempo di pace e quelli in tempo di guerra, sembra – ad avviso di chi scrive – riduttivo operare una netta distinzione tra le ipotesi. Come esaminato in precedenza, infatti, in alcuni casi

---

[22] Si veda SCHMITT M.N., *Tallin*, cit., p. 30.; BLANCO S.M., *Full Protection and Security in International Investment Law*, Svizzera 2019, pp. 375 ss.; *International Law Association*, *Study Group on Due Diligence* in *International Law*, First Report (7 March 2014) p. 2.

[23] Sulla sicurezza cibernetica si veda FARINA M., LUCANIA P., *La sicurezza nella cyber dimension*, Vicalvi 2016, pp. 33 e 61.

[24] Come ha ricordato il Presidente estone in occasione della presentazione del secondo Manuale di *Tallin*, il primo caso in cui le regole proprie del Diritto internazionale hanno trovato applicazione nei casi di attacchi informatici durante un conflitto armato si è avuto nel 2007, quando l'Estonia subì degli attacchi *DoS*.

[25] Anche in questa occasione si ribadisce il carattere politicamente neutrale del gruppo di lavoro e l'impegno di tutti all'obiettività, che impone l'inclusione di tutte le opinioni ragionevoli riguardanti l'interpretazione e l'applicazione del diritto internazionale nel contesto cibernetico. Cfr. *https://ccdcoe.org/research/tallinn-manual/Cfr.*

gli attacchi iniziano in tempo di pace, ma risultano essere prodromici ai successivi attacchi militari in senso stretto, rendendo, così, difficile una loro collocazione all'interno di un gruppo piuttosto che di un altro. Per essere certi di attribuirgli una giusta connotazione, allora, sarebbe più opportuno analizzare non tanto la tipologia di attività, quanto gli effetti e le conseguenze prodotte da tali condotte e, solo nel caso in cui non sia ravvisabile alcun nesso causale con successive operazioni militari, applicare il diritto interno dello Stato che subisce l'attacco.

3. Gli attacchi *Denial of service* e la questione definitoria.

Prima di analizzare nello specifico la normativa italiana applicabile alle ipotesi di attacchi *DoS*, sembra opportuno ripercorrere le possibili definizioni, così da delimitarne il perimetro e individuare i casi che sono da annoverare nella categoria dei reati informatici. Gli attacchi DoS, infatti, danno luogo a ipotesi di delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici; cionondimeno la casistica e le modalità delle condotte sono molto ampie, anche se tutte accomunate da un evento criminoso che si concretizza nell'interruzione di un servizio informatico e/o telematico.

Ne discende che il problema definitorio è ben più ampio e pone questioni anche in termini di rispetto del principio di tassatività e determinatezza, soprattutto in considerazione della problematicità di sussumere le fattispecie concrete a quelle astratte. In tale momento, infatti, alla consueta difficoltà di dover stabilire una perfetta omogeneità tra le due ipotesi, si aggiunge la scarsa intelligibilità delle definizioni tecniche, dovuta proprio all'ampio catalogo.

Un primo profilo di criticità è strettamente connesso alle modalità di commissione dell'attacco, dal momento che questo potrebbe essere perpetrato per il tramite di strumenti che costituiscono al tempo stesso anche il mezzo di commissione di altri reati informatici. Basti pensare ai *virus* o ai *malware* che non necessariamente sono sempre causa di interruzione del servizio ma che possono dare luogo – ad esempio – a una ipotesi di accesso abusivo a un sistema informatico.

Un secondo profilo, invece, riguarda la fluidità delle condotte, che pongono spesso questioni di concorso di norme ovvero di reati, dal momento che possono integrare al contempo ipotesi diverse. È ciò che avviene nel caso di un *DoS* che si consuma dopo aver dato luogo a *un accesso abusivo ad un sistema informatico* ai sensi dell'art. 615 *ter* c.p., o anche alle ipotesi previste dall'art. 617 *quater* c.p. dettato in tema di *intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* [26].

[26] La recentissima L.23.12.2021n. 238 ha riscritto gli artt. articoli 615 *quater*, 615 *quinquies*, 617, 617 *bis*, 617 *quater* e 617 *quinquies*, in risposta all'apertura della procedura di infrazione aperta dalla Commissione europea nei confronti dell'Italia

Volendo trovare una definizione, è necessario fare riferimento alle linee guida dettate nel 2013 dal Comitato della Convenzione sulla criminalità informatica [27], che definiscono i *DoS* come dei malfunzionamenti dovuti a un attacco a causa del quale si esauriscono deliberatamente le risorse di un sistema informatico che fornisce un servizio, fino a renderlo non più in grado di erogare il servizio stesso. Il malfunzionamento può riguardare sia un oggetto informatico materiale, sia un oggetto informatico immateriale [28], a seconda se l'attacco colpisca un apparato come un *hardware* o un *server*, ovvero interrompa un flusso di informazioni come *mail* o scambi di dati di qualsiasi genere. La condotta maggiormente utilizzata per bloccare un servizio, dunque, coincide con l'inondare di traffico dati un *server* di rete, sovraccaricandolo e costringendo il sistema a una continua elaborazione, a seguito della quale si determina il blocco totale. Un simile attacco può anche essere indiretto, come nel caso in cui sia portato contro un *server* o un *cloud*, ripercuotendosi su tutto il traffico dati che utilizza proprio quel *server*.
Le modalità di un attacco *DoS* possono essere anche molto varie [29] e la congestione del traffico dati non è l'unica forma conosciuta. Le interruzioni del servizio possono concretizzarsi, ad esempio, anche nella forma di uno svuotamento della memoria CPU, o determinare una riduzione della potenza di calcolo.

per il mancato recepimento della Direttiva 2013/40/Ue relativa agli attacchi contro i sistemi di informazione. L'intervento normativo ha ampliato il novero delle condotte descritte negli articoli sopra indicati e ha elevato il quadro sanzionatorio, adeguandolo alla cornice edittale, proprio in recepimento di quanto disposto dalla citata Direttiva.

[27] Si tratta delle Linee guida T-CY n. 5 (2013 – 10 E Rev), adottate dal Comitato della convenzione sulla criminalità informatica (T-CY), istituito dal Consiglio d'Europa e che rappresenta le parti della Convenzione di Budapest con la finalità di monitorarne il livello di attuazione. Le linee guida sono state adottate con delibera della nona Plenaria del 5 giugno 2013. Cfr. *https://rm.coe.int/09000016802e9c49*. Per una definizione tecnico-informatico v. SUBRAMANI R., *Denial of Service attacksand mitigation techniques: Real time implementation with detailed analysis*, *White paper of School of Computer Science and Electronic Engineering*, *University of Essex,* 2021, pp. 4 ss.

[28] Cfr. CAPPELLINI A., *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, cit., p. 764. L'autore distingue tra aggressioni materiali e aggressioni logiche.

[29] Per un maggiore approfondimento sulle tipologie di attacco *DoS*, v.*http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-9900/ddos/ddos.htm* e *https://www.cybersecurity360.it/nuove-minacce/moderni-attacchi-ddos-cosa-sono-e-come-mitigarne-i-danni/*.

Queste le ipotesi classiche, ma ci sono anche forme più aggressive di *DoS* come nell'ipotesi del *Permanent Denial of Service*, ovvero del *Distributed Denial of service*.
Nel primo caso, altrimenti detto *Phlashing*, lo scopo è la distruzione dell'*hardware* tramite la sostituzione di un codice o di un programma difettoso (*firmware*), che ne interromperà il funzionamento. Diversamente, nel secondo, l'interruzione del servizio è causato da attacchi multipli da parte di più macchine (*botnet*), che inviando svariati pacchetti di richieste dati, determinano una veloce saturazione del sistema e il suo conseguente malfunzionamento.
Indipendentemente dal tipo di servizio interrotto (sia esso digitale, informatico o telematico) e quale che siano le modalità dell'attacco, i danni prodotti sono considerevoli [30]. Non si tratta solo dei danni diretti che riguardano le apparecchiature e i costi di ripristino dei sistemi, ma è necessario considerare anche i danni indiretti come quelli all'immagine, che determinano la perdita di clienti minando così la fiducia e la sicurezza delle attività digitali, e quelli relativi ai costi da sostenere per garantire la sicurezza dei sistemi.
I casi, oggetto di cronaca, sono sempre più diffusi e i *DoS* colpiscono sia servizi di tipo pubblico sia privato e già all'inizio degli anni Duemila [31] numerosi attacchi interessarono società di tipo commerciale, come Amazon, e società di business, come JPMorgan Chase [32]. Esempi più recenti, avvenuti in Italia, riguardano il caso occorso al Centro elaborazione dati della Regione Lazio, che ha portato all'interruzione di tutti i servizi della piattaforma informatica sanitaria, e il *DoS* che ha impedito il funzionamento del sito di *Eurobet*, la più grande società *online* di giochi e scommesse presente in Italia. Nel primo, l'attacco ha avuto pesanti conseguenze sulla campagna vaccinale in corso, che ha subito rallentamenti e perdite di dati, mentre nel secondo, in cui sono stati coinvolti anche altri *provider* italiani, l'unica soluzione possibile è stata la cancellazione del sito da internet.
Le ragioni poste alla base di tali attacchi sono le più disparate. Nelle maggior parte delle ipotesi le interruzioni di servizio sono intenzionali, come nell'evenienza di richieste di veri e propri riscatti al fine di lucro o come nel

[30] V. S. KRATCHMAN, J.L. SMITH, M. SMITH (a cura di), *The perpetration and prevention of cybercrimes*, in *Internal Auditing*, 2008, Vol. 23, 2, pp. 3-12. Recenti stime hanno calcolato in sei trilioni di dollari l'ammontare annuo mondiale del costo dovuto al *cybercrime* in generale; cfr. *https://www.corrierecomunicazioni.it/cyber-security/il-prezzo-dei-cyberattacchi-nel-mondo-i-danni-toccano-quota-6-trilioni-di-dollari/*.
[31] *Ibidem*.
[32] Per un'ampia panoramica sui casi noti di *Denial of Service* a danno di grandi società, N. K. KATYAL, *Criminal Law in Cyberspace*, *University of Pennsylvania Law Review*, 2001, 149, pp. 26 ss.

caso di lavoratori infedeli disonesti o risentiti. In una parte residuale, invece, il fenomeno non ha una base volontaria, essendo la conseguenza di disastri naturali, piuttosto che di errori o manomissioni colpose. Ebbene, la normazione penale interna, di cui si dirà più avanti, fa riferimento solo alle prime, non avendo il legislatore dato rilevanza alle condotte colpose.

4. L'inquadramento normativo.

In questa sede non è possibile analizzare compiutamente tutti gli interventi normativi che in ambito sovranazionale e nazionale hanno riguardato le innovazioni tecnologiche in generale e la criminalità informatica in particolare. Tuttavia, è necessario – ad avviso di chi scrive – dare conto almeno degli estremi degli atti più significativi, per meglio comprendere l'evoluzione della disciplina e gli scopi di tutela, rinviando alle singole parti della trattazione l'analisi delle innovazioni e modifiche normative.

I mutamenti legislativi recentemente introdotti, infatti, trovano applicazione anche nel caso degli attacchi *DoS*, talvolta con intenti di prevenzione, tal altra con finalità repressive e di contrasto.

Il primo provvedimento in ambito sovranazionale è stato adottato dal Comitato dei Ministri del Consiglio d'Europa, che il 13 settembre 1989 ha stilato la Raccomandazione n. R (89) 9, dettata in tema di criminalità informatica. A seguito di tale atto è scaturita in ambito nazionale la riforma ad opera della L. 23.12.1993 n. 547, con cui furono introdotte nel codice penale le nuove fattispecie del danneggiamento informatico (art. 635 *bis*), le ipotesi di attentato a sistemi, dati, informazioni o programmi informatici di pubblica utilità (art. 420 co. 2 e 3), infine acquisirono rilevanza penale le condotte di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 *quinquies*) [33].

Altre pietre miliari in tema di criminalità informatica sono state la Convenzione del Consiglio d'Europa, firmata a Budapest il 23 novembre 2001e attuata in ambito nazionale con la L.18.03.2008n. 48, e la Decisione quadro del Consiglio dell'Unione europea 2005/222/GAI [34].

In particolare, la legge di ratifica del 2008 ha apportato modifiche sostanziali alle fattispecie dettate in tema di danneggiamento informatico (artt. 635 *bis*, *ter*, *quater* e *quinquies* c.p.), recependo anche la distinzione tra integrità dei

[33] Per una più compiuta analisi delle riforme, CAPPELLINI A., *I delitti*, cit., pp. 768 ss., che ricorda l'ulteriore modifica ad opera del legislatore del '93 in tema di equiparazione della violenza informatica sulle cose a quella fisica (art. 392 ult. co. c.p.).

[34] In *https://www.coe.int/it/web/conventions/full-list?module=treaty-detail&treatynum=185* e in *https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32005F0222*.

dati e integrità del sistema, oltre che prevedendo una disciplina *ad hoc* nei casi in cui l'oggetto della tutela abbia rilevanza a fini pubblicistici.
Un importante approdo normativo in tema di contrasto alla criminalità informatica in forma preventiva è costituito dalla Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante *misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*. Il provvedimento riguarda, nello specifico, la tutela della *cybersecurity* e si applica agli operatori di servizi essenziali e di servizi digitali, tenuti ad adottare adeguate misure per la prevenzione degli incidenti e degli attacchi informatici per non incorrere nel severo trattamento sanzionatorio predisposto. È, altresì, previsto che ogni Stato debba dotarsi di un gruppo di intervento nazionale, che avrà un corrispettivo anche in ambito sovranazionale.
Ci sono, poi, un gruppo di norme di rango sovranazionale che non hanno una incidenza diretta sulle condotte penalmente rilevanti in tema di *DoS*, ma che devono essere tenute in conto rispetto all'oggetto della tutela prevista, come nel caso del Regolamento (UE) 2016/679 e della Direttiva (UE) 2016/680[35]. La tutela dei dati in generale, infatti, potrebbe venire in rilievo anche quando condotte di interruzione dei servizi e dei sistemi informatici possano determinare la perdita di tali dati.
Anche in ambito nazionale alcuni recenti interventi del legislatore potrebbero avere punti di contatto con le fattispecie previste in tema di attacchi *DoS*, come – ad esempio – nel caso del D.lgs. 08.11.2001n. 184, che attua la Direttiva (UE) 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e rispetto al quale potrebbero delinearsi ipotesi di concorso di norme e/o di reati. Basti pensare all'ipotesi in cui la diffusione di un *virus*, ad esempio, sia finalizzato a interrompere un servizio informatico e a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 *quater* c.p.), ovvero dia luogo a un concorso con l'ipotesi della frode informatica nella nuova versione prevista nell'art. 640 *ter* co. 2 c.p.
Il tema della *cybersecurity* è al centro dell'agenda di governo, tant'è che già nel 2017 è stato approvato un piano nazionale di rafforzamento della sicurezza e sono stati istituiti alcuni organi con competenze specifiche, come il Comitato interministeriale per la sicurezza della Repubblica (CISR), il Dipartimento delle informazioni per la sicurezza (DIS), il Nucleo sicurezza

[35] Si tratta nel primo caso del Regolamento dettato in tema di protezione dei dati personali (GDPR) e della Direttiva del Parlamento europeo e del Consiglio relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

cibernetica (NSC), nonché l'Agenzia per l'Italia digitale (AGID)[36]. Recentemente, poi, il d.l. n. 82/2021 ha istituito l'Agenzia per la cybersicurezza nazionale, stabilendo articolatamente competenze e compiti al fine di proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico[37].

5. La disciplina codicistica.

I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici non costituiscono una categoria autonoma, tant'è vero che non godono neanche di una collocazione unitaria all'interno del codice penale. Piuttosto, è necessario rifarsi, di volta in volta, a singole disposizioni introdotte dal legislatore nel tempo [38], con un *modus operandi* che evidenzia la mancata armonizzazione delle norme e solleva dubbi in merito al rispetto dei principi di ragionevolezza e proporzione, come si vedrà più avanti.

Rispetto alla Convenzione di Budapest del 2001, gli artt. 4 e 5 richiedono agli Stati di introdurre rispettivamente le fattispecie di *attentato all'integrità dei dati* e *attentato all'integrità di un sistema*, ossia una fattispecie che sanzioni *il danneggiamento, la cancellazione, il deterioramento, la modifica o la soppressione di dati informatici senza autorizzazione*, e una norma che punisca *il serio impedimento senza alcun diritto, del funzionamento di un sistema informatico*, qualora questo si verifichi a seguito di condotte di *introduzione, trasmissione, danneggiamento, cancellazione, deterioramento, alterazione o soppressione di dati informatici*.

Solo con la legge di ratifica della Convenzione il legislatore italiano ha scisso le due ipotesi [39], disciplinando all'art. 635 *bis* c.p. la fattispecie di danneggiamento di informazioni, dati e programmi informatici, mentre all'art. 635 *quater* c.p. l'ipotesi del danneggiamento di sistemi informatici o telematici. Proprio in quest'ultima norma si inquadrano, tendenzialmente, i casi di *DoS*, intesi come attacchi al funzionamento di un sistema informatico

[36] In *https://docs.italia.it/AgID/documenti-in-consultazione/lg-cert-regionali/it/bozza/contesto.html*.

[37] Si tratta del d.l. 14 giugno 2021 n. 82 convertito con modificazioni nella legge 4 agosto 2021 n. 10 recante *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*. Per una descrizione delle competenze e funzioni si veda MARRONE A., SABATINO E., CREDI O., *L'Italia e la difesa cibernetica,* in *https://www.iai.it/sites/default/files/iai2112.pdf, p. 7 ss*.

[38] PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI - S. CANESTRARI - A. MANNA - M. PAPA (A cura di), *Cybercrime*, cit., pp. 71 ss.

[39] Una più puntuale descrizione degli elementi della fattispecie si avrà più avanti.

o telematico. Cionondimeno, nella comparazione tra le norme si ravvisa una differenza non di poco conto, laddove nelle disposizioni convenzionali, tra le condotte sanzionabili, non è annoverata l'ipotesi della distruzione. Sono previste, infatti, solo le ipotesi del deterioramento o danneggiamento, che, tuttavia, non implicano necessariamente un blocco totale dei dati o del sistema, potendo residuarne una parte ancora funzionante e ripristinabile a mezzo di interventi tecnici. Diversamente, la distruzione lascia intendere che il sistema sia del tutto demolito, senza possibilità di utilizzo alcuno.
Il legislatore italiano, poi, ha introdotto gli artt. 635 *ter* e *quinquies* c.p., per le ipotesi in cui le condotte ora descritte coinvolgano informazioni, dati, sistemi informatici o telematici utilizzati dallo Stato o da altro ente pubblico, ovvero siano di pubblica utilità [40].
Sin qui l'ambito codicistico è quello dei reati contro il patrimonio, ma rispetto al bene giuridico non tutti concordano e trova sempre più consenso l'orientamento secondo cui proprio l'integrità dei dati, programmi e sistemi informatici costituisca essa stessa il bene giuridico tutelato [41]. L'esigenza di individuare un nuovo bene giuridico scaturirebbe anche dalla considerazione che le condotte sanzionate non necessariamente determinano un danno patrimoniale, ben potendo – ad esempio – la perdita dei dati essere risolta grazie a copie di *backup* [42]; non solo, ma un simile argomentare permetterebbe di individuare un unico bene giuridico per tutte le fattispecie in esame. Diversamente, ove prevalesse la concezione patrimonialistica, si porrebbe una frattura rispetto alle ipotesi di danneggiamento di dati e sistemi informatici pubblici, per le quali prevarrebbe la dimensione pubblicistica e il bene oggetto di tutela coinciderebbe con l'ordine pubblico [43].
Rispetto ai delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici, vengono in rilievo anche le condotte prodromiche sanzionate ai sensi dell'art. 615 *quinquies* c.p. ed è qui che si evidenzia il corto circuito degli interventi normativi in tema di reati informatici. La norma, infatti, punisce *chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del*

---

[40] V. anche, PERFETTI T., *I crimini informatici*, in BASSOLI E. (A cura di), *I crimini informatici, il dark web e le web room*, Pisa 2021, pp. 155-161.
[41] Cfr. PICOTTI L., *Sistematica dei reati informatici, Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in PICOTTI L. (A cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova 2004, pp. 70 ss.
[42] V. CAPPELLINI A., *I delitti*, cit., p. 777.
[43] Per una critica a tale ricostruzione, SALVADORI I., *Il microsistema normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. It. Dir. Proc. Pen.*, 2012, 1, p. 239.

suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri, installa apparecchiature, dispositivi o programmi informatici [44], collocando tali ipotesi nell'ambito dei reati contro la persona e, in particolare, dei reati contro l'inviolabilità del domicilio. Dunque, diffondere un *virus* senza che ciò determini necessariamente una ipotesi di interruzione del sistema dà luogo a una fattispecie in cui il bene giuridico tutelato è di rango superiore – trattandosi di un reato contro la persona –, ma la cui condotta è sanzionata meno severamente, rispetto a quelle che realizzano una vera e propria interruzione di un servizio, che costituirebbero *solo* una ipotesi di reato contro il patrimonio, seppure punita in misura maggiore [45].
Pur non costituendo il *quantum* di pena un *discrimen* rilevante, sembra opportuno un ripensamento in merito alla collocazione sistematica delle fattispecie in esame all'interno del codice, ma con ogni probabilità una valutazione circa l'opportunità di raggruppare in un unico *corpus* di norme tutta la materia della criminalità informatica [46]. Ciò permetterebbe, così, di superare le obiezioni poste rispetto ai criteri di ragionevolezza e proporzione soprattutto sotto il profilo del trattamento sanzionatorio.

6. Le fattispecie previste dagli artt. 635 *bis*, *ter*, *quater* e *quinquies* c.p.
Si tratta di un gruppo di norme accomunate dall'intenzione del legislatore di punire il danneggiamento, ma che presentano alcune differenze, in particolare per l'oggetto e per la qualità del suo titolare, ma non solo.
Sotto il primo profilo, negli artt. 635 *bis* e *ter* c.p. la sanzione colpisce l'ipotesi del danneggiamento di informazioni, dati e programmi informatici, ossia di beni immateriali [47] del tutto privi di una dimensione fisica e, peraltro, di difficile definizione. La Convenzione sulla criminalità informatica definisce solo il dato informatico, chiarendo che si tratta di una *qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione* [48]. Il dato, allora, costituirebbe una entità minima che aggregato in più unità darebbe

[44] Anche questa norma è stata oggetto di riforma ad opera della L. 23.12.2021 n. 238 recante *Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea* (cd. Legge europea 2019-2020). Si rinvia alla nota n. 2.
[45] Nel primo caso la sanzione reclusione fino a due anni e con la multa sino a euro 10.329, mentre nel secondo, reclusione da uno a cinque anni.
[46] Cfr. FUMO M., *La condotta nei reati informatici*, in *Arch. Pen.*, 2013, 3, p. 774.
[47] V. FIANDACA G., MUSCO E., *Diritto penale. Parte speciale*, Bologna 2014, II, p. 147.
[48] Art. 1 lett. b Convenzione del Consiglio d'Europa sulla criminalità informatica, Budapest 23 novembre 2001.

luogo a una informazione intelligibile da parte dell'utente. Diversamente, il programma informatico è composto da una serie di istruzioni che possono essere eseguite da un sistema informatico per la risoluzione di un determinato problema [49].

Negli artt. 635 *quater* e *quinquies*, invece, l'oggetto materiale del reato coincide con i sistemi informatici o telematici. Sulla questione definitoria viene ancora una volta in aiuto l'art. 1 della Convenzione di Budapest, secondo cui si deve intendere per sistema informatico *qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati*. Invero, la norma convenzionale non fa riferimento alcuno ai sistemi telematici, ma ciò non significa che l'ambito di tutela sia diverso rispetto a quanto predisposto dal legislatore italiano. I sistemi telematici, infatti, fanno riferimento alle telecomunicazioni e, dunque, al mondo di internet, rispetto al quale i sistemi informatici (computer ed elaboratori anche connessi tra loro per lo scambio di dati) in passato non erano necessariamente collegati. L'attuale sviluppo tecnologico, invece, porta a ritenere assorbito l'ambito telematico in quello informatico, dal momento che è difficilmente immaginabile – almeno nell'uso comune – un computer non sempre connesso al *web*.

Sotto il profilo della qualifica del titolare del bene giuridico, mentre gli artt. 635 *bis* e *quater* riguardano ipotesi in cui il danneggiamento colpisce informazioni, dati, programmi e sistemi in uso a soggetti privati, gli artt. 635 *ter* e *quinquies* c.p. fanno riferimento al caso in cui gli stessi oggetti giuridici siano utilizzati dallo Stato o da altro ente pubblico, ovvero abbiano comunque una pubblica utilità. Non è necessaria, dunque, una qualifica pubblica formale, dal momento che il coefficiente minimo richiesto dalla norma è il valore di pubblica utilità dell'oggetto materiale, posto il considerevole numero di utenti che possono subire danni da tali condotte e la dimensione pubblicistica della funzione assicurata dall'uso di tali oggetti.

Ciò giustifica anche un trattamento sanzionatorio piuttosto severo, pur con qualche elemento di incoerenza. Il danneggiamento di dati, informazioni e programmi di pubblica utilità è, infatti, punito più severamente dell'ipotesi corrispettiva in cui i titolari sono soggetti privati, e la stessa pena è prevista anche per il danneggiamento di sistemi informatici o telematici di pubblica utilità. Tuttavia, in quest'ambito la sanzione è inspiegabilmente minore rispetto all'ipotesi corrispettiva prevista a tutela dei privati [50].

[49] Cfr. MANTOVANI F., *Diritto penale. Parte speciale*, Padova, 2021, II, pp. 145 ss.

[50] Non manca in dottrina chi ritiene irragionevoli e sproporzionate per eccesso le sanzioni previste. Riporta il dibattito CAPPELLINI A., *I delitti*, cit., p. 807.

Per quanto concerne il soggetto agente, tutte le fattispecie in esame danno luogo a reati comuni, non essendo richiesta nessuna qualifica particolare e potendo chiunque porre in essere le condotte descritte.
Per quanto attiene all'elemento dell'evento, gli artt. 635 *bis* e *quater* c.p. contemplano la produzione del danno affinché operi la punibilità in capo al reo, ma gli artt. 635 *ter* e *quinquies* c.p. sono costruiti secondo lo schema dei reati di attentato [51], essendo sufficiente che il soggetto compia fatti diretti a causare uno degli eventi previsti dal dettato normativo.
Proprio in riferimento alla produzione dell'evento, l'orientamento dominante ritiene vi sia una sostanziale coincidenza tra gli eventi e le condotte descritte nelle fattispecie, anzi la distruzione, il deterioramento, la cancellazione, l'alterazione e la soppressione costituirebbero gli eventi prodotti da condotte sostanzialmente libere [52]. Attenendosi al dato formale circa le tipologie di condotte ricomprese nel dettato normativo, è necessario distinguere a seconda se ci si riferisce al danneggiamento di informazioni, dati e programmi informatici, ovvero al danneggiamento di sistemi informatici o telematici. Nel primo caso, accanto alle condotte proprie del danneggiamento tradizionale, si aggiungono condotte tipiche dell'ambito informatico per un totale di cinque tipologie diverse. In particolare, distruzione e deterioramento – mutuati dall'art. 635 c.p. – concernono i casi in cui l'oggetto materiale sia completamente annientato o sia modificato in senso peggiorativo e dunque compromesso nella sua funzionalità [53]. Le condotte di cancellazione, alterazione e soppressione, invece, fanno riferimento alle ipotesi in cui la modifica o la manipolazione dell'oggetto giuridico siano finalizzate alla sua eliminazione, con l'unica differenza rimarcabile che la cancellazione è più facilmente riferibile alle informazioni, mentre l'alterazione e la soppressione ai dati e ai programmi [54].
Relativamente alle condotte previste nella fattispecie di danneggiamento di sistemi informatici o telematici *ex* art. 635 *quater* c.p., la norma opera un richiamo a quanto previsto dall'art. 635 *bis* c.p. e aggiunge le ipotesi dell'introduzione, o trasmissione di dati, informazioni e programmi. Sennonché, anche qui emerge la materiale e tautologica sovrapposizione tra le condotte descritte nell'art. 635 *bis* c.p. e poi richiamate nell'art. 635 *quater* c.p. e gli eventi di distruzione, danneggiamento, inservibilità dei sistemi informatici o telematici successivamente indicati. Infine, un'ultima ipotesi è prevista per il cd. *sabotaggio informatico*, che si ha quando le condotte indicate determinano un grave ostacolo al funzionamento del sistema. È

[51] Sulla configurazione come reati di attentato v. infra § 5.
[52] V. PICOTTI L., *La ratifica della Convenzione Cybercrime. Profili di diritto penale sostanziale*, in *Dir. Pen. Proc.*, 2008, 6, pp. 713 ss.
[53] Cfr. FIANDACA G., MUSCO E., *Diritto*, cit., p. 142.
[54] Cfr. CAPPELLINI A., *I delitti*, cit., p. 787.

proprio questo il caso dei *DoS*, ossia degli attacchi che interrompono il funzionamento di un servizio, per i quali il requisito della gravità permette di escludere dalla fattispecie ipotesi non particolarmente offensive come l'invio di *mail spam*[55].
Circa l'elemento soggettivo, le norme esaminate richiedono il dolo generico, da intendersi nel senso della coscienza e volontà del fatto tipico così come descritto dal legislatore.
Rispetto alla compatibilità di tali fattispecie con l'istituto del tentativo, è necessario operare una distinzione. Le ipotesi disciplinate dagli artt. 635 *bis* e *quater* c.p. danno luogo a reati di evento, per i quali è possibile che il soggetto agente ponga in essere atti idonei e diretti in modo non equivoco a distruggere, deteriorare, cancellare, alterare o sopprimere, introdurre o trasmettere, senza che senza che l'azione si compia o l'evento si verifichi. Per le ipotesi, invece, previste dagli artt. 635 *ter* e *quinquies* c.p., il tentativo non è configurabile, trattandosi di reato di attentato.

7. Il regime delle circostanze aggravanti.
L'intervento di depenalizzazione ad opera del D.lgs. 15.01.2016 n. 7, che ha modificato la fattispecie tradizionale del danneggiamento contenuta nell'art. 635 c.p. degradandola a illecito civile e mantenendo rilevanza penale alla sola ipotesi del danneggiamento aggravato dalla violenza o minaccia, ha modificato anche i delitti cd. di danneggiamento informatico. Questi, infatti, sono stati costruiti secondo il modello proprio del danneggiamento classico, sicché si è reso necessario introdurre in tutte e quattro le fattispecie un comma contenente la previsione della violenza alla persona o minaccia e, in aggiunta, l'abuso della qualità di operatore del sistema.
L'intervento legislativo, dunque, non ha modificato in maniera sostanziale le norme, pur tuttavia è stato da più parti rilevato un aumento della già segnalata sproporzione nel trattamento sanzionatorio tra le ipotesi di danneggiamento informatico da un lato, e di danneggiamento ordinario dall'altro [56]. A seguito della riforma, infatti, la sanzione prevista dall'art. 635 c.p. è la reclusione da sei mesi a tre anni, mentre nell'art. 635 *bis* c.p. comminata è la reclusione da uno a quattro anni.
Nonostante la circostanza aggravante introdotta nei delitti in esame sia la stessa per tutte le ipotesi, l'aumento di pena è indicato solo nel primo caso, mentre negli altri il *quantum* non è stabilito. Si tratterebbe, dunque, di circostanze a effetto comune, per le quali l'aumento deve essere calcolato fino a un terzo rispetto all'ipotesi base. Le tre diverse ipotesi circostanziate potrebbero concorrere tra loro ed essere contestate in maniera simultanea, con la conseguenza che il giudice – ai sensi dell'art. 63 comma 2 c.p. – dovrà

[55] Cfr. SALVADORI I., *Il microsistema*, cit., pp. 204 ss.
[56] Cfr. CAPPELLINI A., *I delitti*, cit., p. 776.

calcolare una prima variazione sulla pena del reato base, per poi applicare le ulteriori variazioni sull'entità così ottenuta.
In riferimento ai concetti di violenza o minaccia, che pur trattandosi di materia informatica non si discostano dalle previsioni classiche del diritto penale, si pone senz'altro un problema di operatività in concreto. Oltre le ipotesi di danneggiamento a seguito dell'impiego di *vis corporis* sui supporti informatici materiali come computer, memorie esterne *et similia*, è difficile immaginare che l'aggravante abbia un ampio campo di applicazione, nella misura in cui la maggior parte delle condotte descritte dalle norme sono poste in essere da remoto o via *internet* [57].
L'aggravante dell'abuso della qualità di operatore del sistema è stata prevista in considerazione della particolare posizione rivestita dal soggetto agente, nella misura in cui la sua maggiore conoscenza informatica si tramuta in un più alto rischio per i dati, i programmi e i sistemi informatici.
Rispetto all'inquadramento della figura dell'operatore, questa può essere intesa secondo l'accezione tecnica dell'informatico puro, dell'amministratore del sistema informatico, ovvero prescindendo dalla formazione del soggetto agente e ritenendo tale tutti coloro che hanno mansioni inerenti agli oggetti di cui sopra [58].
Giova sottolineare che gli artt. 635 *ter* e *quinquies* c.p. contengono un secondo comma che potrebbe trarre in inganno. Il legislatore del 2008, infatti, ha previsto un consistente aumento di pena nel caso in cui, dalle condotte principali descritte nel comma precedente derivi, per l'art. 635 *ter* c.p. *la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici*, per l'art. 635 *quinquies* c.p. *la distruzione, il danneggiamento, o l'inservibilità totale o parziale del sistema informatico o telematico*. Mentre nel primo caso c'è una perfetta coincidenza tra le condotte descritte nel primo comma e quelle previste dal secondo, non si può dire la stessa cose per l'ipotesi dell'art. 635 *quinquies* c.p., in cui manca – senza una ragione evidente – il richiamo alla condotta dell'ostacolare gravemente il funzionamento del sistema.
Di primo acchito, la natura giuridica di tali previsioni sembrerebbe essere quella di una circostanza aggravante. Sennonché, la presenza dell'evento di danneggiamento di dati, informazioni, programmi e sistemi informatici e telematici, contenuto negli artt. 635 *ter* co. 2 e *quinquies* co. 2 c.p. rinvia alla figura dei reati aggravati dall'evento, nella specie dei reati di attentato [59].

[57] V. SALVADORI I., *Il microsistema*, cit., p. 236, secondo cui al massimo sarebbe possibile configurare l'ipotesi della minaccia a distanza.
[58] V. BORRUSSO R., BUONOMO G., CORASANNITI G., D'AIETTI G., *Profili penali dell'informatica*, Milano, 1994, p. 90.
[59] Per una ricostruzione dommatica dei reati aggravati dall'evento, FIANDACA G., MUSCO E., *Diritto*, cit., pp. 691 ss.; MANTOVANI F., *Diritto*, cit., pp. 399 ss.

Invero, non manca in dottrina chi riconduce le ipotesi in esami a fattispecie autonome, in base alla considerazione che l'evento appena descritto *è già oggetto del dolo del fatto base del primo comma* [60]. In entrambi i casi, le ipotesi normative sarebbero sottratte al giudizio di bilanciamento tra circostanze[61].

8. Questioni in tema di concorso di norme e di reati.

La tematica necessita di essere esaminata lungo due diverse direttrici di indagine, a seconda se si indaghino i rapporti interni tra le fattispecie di danneggiamento, ovvero si guardi ai rapporti tra le fattispecie di danneggiamento e altri reati.

In merito al primo profilo, i delitti di danneggiamento sono disciplinati secondo la logica propria della progressione criminosa e si caratterizzano per la presenza di una clausola di sussidiarietà espressa, che manca nell'ultima e più grave ipotesi prevista dall'art. 635 *quinquies* c.p. Alcuni ritengono che alla base delle intenzioni del legislatore ci sia la precisa scelta di impedire che si potesse configurare un concorso proprio tra le stesse fattispecie di danneggiamento [62], benché si debba ritenere che il criterio della sussidiarietà operi anche al di fuori del *microsistema dei danneggiamenti informatici* [63], ad esempio in riferimento ad alcune più gravi ipotesi di delitti contro l'incolumità pubblica.

Quanto ai rapporti tra l'ipotesi prevista dall'art. 635 c.p. e le successive fattispecie dettate in tema di delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici, si tratterebbe di un concorso apparente di norme, risolto proprio ai sensi dell'art. 15 c.p., in cui gli artt. 635 *bis* e ss. c.p., pur regolando la stessa materia, presentano elementi di specialità per aggiunta rispetto all'ipotesi tradizionale di danneggiamento, prevalendo sull'applicazione di quest'ultima.

Rispetto al secondo profilo, viene in rilievo dapprima il rapporto tra i reati in esame e il delitto di accesso abusivo a un sistema informatico *ex* art. 615 *ter* c.p. co. 2 nn. 2 e 3. Secondo un primo orientamento troverebbe applicazione il criterio di specialità, a seguito del quale i casi di danneggiamento informatico sono da ritenersi assorbiti. La soluzione non è accolta unanimemente dalla dottrina, nella misura in cui in luogo del criterio di specialità, troverebbe applicazione la disciplina del concorso formale di reati

---

[60] Cfr. SALVADORI I., *Il microsistema*, cit., pp. 232-233.

[61] La giurisprudenza è di altro avviso, avendo affermato in alcune pronunce recenti la natura di fattispecie circostanziata in capo ai reati aggravati dall'evento. Così, Cass. Pen. Sez. I, sentenza 19 novembre 2015 n. 7941. Cfr. MASERA L., *La sentenza della Cassazione sul caso Eternit: analisi critica e spunti di riflessione*, in *Riv. It. Dir. Proc. Pen*., 2015, 3, pp. 1565.

[62] V. CAPPELLINI A., *I delitti*, cit., p. 795.

[63] L'espressione è di SALVADORI I., *Il microsistema*, cit.

nelle ipotesi di danneggiamento doloso, mentre opererebbe l'art. 615 *ter* co. 2 c.p. nei casi di danneggiamento non voluto [64]. Nello stesso senso si è espressa anche la giurisprudenza rispetto a un caso in cui il soggetto agente, per interrompere il funzionamento di una casella di posta elettronica, ha posto in essere una condotta di accesso abusivo modificando le credenziali di accesso [65].

Soluzione opposta per il caso previsto dall'art. 615 *quinquies*, che nel prevedere le ipotesi di chi allo scopo di *danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici*, fa riferimento a condotte che sono prodromiche a quanto stabilito negli artt. 635 *bis* e seguenti. È il caso, ad esempio, del soggetto agente che diffonde un *virus* con la finalità di danneggiare un sistema informatico, senza che lo scopo sia raggiunto. Ove ciò accadesse, infatti, si realizzerebbero le condotte previste nelle norme in tema di danneggiamento e che dunque assorbirebbero proprio le condotte prodromiche.

Infine, viene in rilievo il rapporto tra l'art. 635 *quinquies* c.p. e l'art. 420 c.p. relativo alle ipotesi di attentato a impianti di pubblica utilità, in cui la prima fattispecie è speciale – e dunque prevalente – rispetto alla seconda.

Le esigenze di contrasto alla criminalità informatica e di attuazione della disciplina sovranazionale hanno determinato il legislatore a introdurre nel 2008 i reati di danneggiamento informatico, mentre sino ad allora l'art. 420 c.p. trovava larga applicazione anche nei casi di attentato ai sistemi informatici di pubblica utilità. La disposizione, infatti, dedicava i commi 2 e 3 proprio ai sistemi e impianti informatici o telematici, alle informazioni, ai dati e ai programmi, poi abrogati contestualmente all'introduzione degli artt. 635 *bis* e ss.

Nei rapporti tra le ipotesi di danneggiamento informatico e le fattispecie previste dagli artt. 617 *quater*, *quinquies* e *sexies* c.p. dettati a garanzia della libertà e segretezza delle comunicazioni informatiche e telematiche, trova applicazione il concorso formale di reati. I due gruppi di norme non darebbero luogo a una ipotesi di concorso apparente di norme per due ordini di ragioni. Da un lato, infatti, gli elementi tipizzanti le fattispecie sono tra loro diversi, escludendo, pertanto, la possibilità di individuare elementi specializzanti. Dall'altro, in riferimento alla trasmissione dei dati e delle comunicazioni, le disposizioni farebbero riferimento a due diversi momenti:

[64] Riporta il dibattito CAPPELLINI A., *I delitti*, cit., pp. 796 ss.

[65] Così Cass. Pen sez. V, sentenza 25 marzo 2019 n. 18284.

statico per i delitti di danneggiamento informatico, dinamico per quelli di tutela delle comunicazioni [66].

Il concorso formale di reati ricorre anche in riferimento alle ipotesi in cui con una condotta di danneggiamento si realizzi pure una condotta di frode informatica ai sensi dell'art. 640 *ter* c.p. [67]. Le due fattispecie, infatti, presentano una diversità di struttura tale da escludere il rapporto di specialità, laddove nel primo caso al sistema informatico è impedito il funzionamento, mentre nel secondo esso continua a funzionare, pur se in modo alterato. Basti pensare al caso in cui il soggetto agente sferri un attacco *DoS*, interrompendo ad esempio un servizio bancario *online*, e al contempo riesca a procurare a sé o ad altri un ingiusto profitto con altrui danno chiedendo il pagamento di una somma di denaro per ripristinare il sistema, ovvero riuscendo a utilizzare carte di credito altrui, entrando in possesso e di dati e *password*.

Più problematico l'inquadramento dei rapporti tra le fattispecie di danneggiamento informatico e l'ipotesi prevista dall'art. 392 co. 3 c.p. dettato in tema di *esercizio arbitrario delle proprie ragioni con violenza sulle cose* [68]. Quest'ultima norma si colloca nell'ambito dei delitti contro l'amministrazione della giustizia e fa riferimento alle condotte di alterazione, modificazione, cancellazione totale o parziale di un programma informatico, ovvero di impedimento o turbamento del funzionamento di un sistema informatico o telematico. La presenza del dolo specifico individuato nel fine di *esercitare un preteso diritto*, porta a escludere la configurabilità di una ipotesi di concorso con le fattispecie di danneggiamento e a ritenere del tutto residuale l'operatività dell'art. 392 co. 3 c.p., rispetto ai casi in cui la violenza sulla cosa informatica sia già tipizzata in maniera autonoma e speciale [69].

---

[66] Cfr. MANNA A., DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'internet provider*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (A cura di), *Cybercrime*, cit., p. 931.

[67] Il delitto di frode informatica è stato oggetto di un recente intervento normativo ad opera della D. lgs. 8 novembre 2021 n. 184, entrato in vigore il 14 dicembre 2021 in attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti.

[68] Non è questa la sede per riportare tutto il dibattito sull'equiparazione tra la violenza informatica e la violenza sulle cose. Per un'approfondita analisi si rinvia a CAPPELLINI A., *I delitti*, cit., p. 818.

[69] *Ibidem*, p. 819. E', appunto il caso dei delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici.

9. Alcuni rilievi conclusivi.

Trovandoci nell'era della quarta rivoluzione industriale [70], è innegabile che la materia dei reati informatici acquisisca sempre più un ruolo di primo piano anche nell'ambito del sistema penale. In tema di danneggiamento informatico, e in particolare di *Denial of Service*, si è portati a immaginare per lo più le ipotesi in cui la finalità perseguita dal reo è quella di ottenere un ingiusto profitto, o i casi di pratiche commerciali scorrette. Questa visione è agevolata nel nostro ordinamento dalla scelta di politica criminale del legislatore di collocare tali reati nell'ambito dei delitti contro il patrimonio.

Pur tuttavia, c'è un fenomeno sommerso e ancora poco noto, relativo agli attacchi *DoS* perpetrati da alcuni Stati a danno di altri, in una sorta di guerra informatica che, in assenza di una normativa internazionale di riferimento, meglio si collocherebbe nell'ambito dei reati contro la personalità dello Stato, o – in alcuni casi – dei delitti contro l'ordine pubblico[71].

Nella guerra del *cyberspazio* non ci sono vittime umane, bensì attacchi all'economia in tempi di pace e alla sicurezza in tempi di guerra ed è questo il motivo per cui molti Stati chiedono a gran voce che tutta la materia sia oggetto di accordi internazionali[72]. Ciò permetterebbe un'armonizzazione delle singole legislazioni nazionali in materia, la cui efficacia, peraltro, è condizionata fortemente dalla dimensione transfrontaliera dei reati. La dimensione di *a-territorialità*, infatti, pone questioni anche in termini di *locus commissi delicti*, che a livello sovranazionale sono state affrontate dalla Decisione quadro 2005/222/GAI [73]. Il provvedimento all'art. 10 ha previsto che per stabilire la competenza giurisdizionale di ogni Stato devono ricorrere uno dei seguenti parametri: il reato è stato commesso in tutto o in parte sul

---

[70] Cfr. FLORIDI L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano 2017.

[71]Cfr. BROWN I., EDWARDS L., MARSDEN C.T., *Information Security and Cybercrime*, in EDWARDS L., WAELDE C. (a cura di), *Law and the internet*, eds. Oxford: Hart, 2009, *passim*. Nell'ambito degli attacchi a danno dei sistemi informatici sferrati in occasione dei conflitti bellici, come quello in corso in Ucraina e finalizzati a interferire con l'organizzazione della difesa e a destabilizzarne il potere politico e militare, spesso le condotte sono poste in essere da entrambe le parti, e, infatti, nel conflitto citato l'Ucraina ha subito inizialmente tali attacchi, tuttavia – successivamente - una rete di attivisti che vanno sotto il nome di Anonymous ha lanciato attacchi *DoS* contro i siti del Cremlino e delle forze armate russe. Cfr. ANNUNZIATA M., *Tra Russia e Ucraina c'è anche il fronte del cyberwarfare*, in *www.treccani.it* e BAIARDI F., *Guerra Ucraina, ecco i danni dei malware distruttivi e le contromisure urgenti*, in *www.cybersecurity360.it*.

[72] Cfr. LIN T. C. W., *Financial Weapons of War*, in *Minnesota Law Review*, 2016, 100, p. 1377.

[73] Si tratta della Decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione, in *https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32005F0222*.

territorio dello Stato, il soggetto agente è un suo cittadino, il reato è stato commesso a beneficio di una persona giuridica che ha sede legale nel territorio dello Stato [74].

Tirando le fila del discorso, in tema di delitti informatici emerge sempre più la necessità di un intervento a livello internazionale, di un rafforzamento dei provvedimenti sovrannazionali e, in ultimo, di un intervento sostanziale da parte del legislatore nazionale. A tal proposito, una rivisitazione di tutta la materia si rende necessaria non solo in termini di collocazione sistematica come accennato sopra, ma richiederebbe anche un superamento almeno parziale di alcune categorie giuridiche classiche. Il *cybercrime* in generale è caratterizzato da una certa fluidità che poco si coniuga, ad esempio, con il concetto tradizionale di azione, in cui l'unicità o meno delle condotte non è sempre facilmente tracciabile e il cui segno emerge in maniera evidente dalla difficoltà del legislatore di distinguere – nelle fattispecie esaminate – tra l'oggetto materiale e le condotte stesse.

La scelta di raggruppare tutta la categoria dei reati informatici in un unico *corpus* normativo permetterebbe di graduare meglio il trattamento sanzionatorio, superando anche le obiezioni mosse in termini di sproporzione delle sanzioni.

Rimane la difficoltà per il diritto di stare al passo con una evoluzione tecnologica estremamente veloce, che rende ardua la possibilità di garantire una disciplina aggiornata e soprattutto efficace.

[74] Il secondo paragrafo dell'art. 10 specifica che il reato è commesso sul suolo dello Stato quando è stato compiuto da una persona fisicamente presente sul territorio e indipendentemente dal luogo in cui sono ubicati i sistemi informatici attaccati, ovvero se il reato è stato commesso ai danni di un sistema informatico ubicato sul territorio dello Stato e indipendentemente dal luogo in cui si trova il reo.