Considerazioni introduttive.

Lo sviluppo delle comunicazioni telematiche e delle nuove tecnologie digitali ha prodotto grandi cambiamenti nelle dinamiche dei rapporti umani. L'era tecnologica e della comunicazione per eccellenza ignora le sfumature morali, crea il *web* ossia un ambiente in cui la dimensione spazio-tempo-individuo si annulla. Le aspirazioni umane, tradotte in algoritmi, trovano nella *rete*, entità astratta ma pervasiva, la moderna Agorà. In questa piazza tutte le istanze sembrano trovare una pronta risposta, ma il *Cyberspace* è anche un luogo infido e temibile.

Il *Cyberspace*, moderno Giano[1], è, sì, portatore del nuovo, ma anche fertile terreno per il pullulare di fatti illeciti nuovi che si affiancano a quelli già noti nel panorama giuridico. L'impressionante velocità dello sviluppo tecnologico è doppiata sul binario parallelo dell'uso illecito. L'affinamento delle tecniche informatiche viene adattato, con pari rapidità, alle nuove forme di criminalità. Da quell'ambiente, virtuale e all'apparenza innocuo e democratico, provengono quindi poderosi attacchi alla *privacy*, all'economia, alle infrastrutture critiche, nonché alla sicurezza sociale. Si potrebbe chiosare: per ogni nuovo strumento tecnologico al servizio dell'umanità c'è una nuova forma di criminalità pronta a distorcere a proprio vantaggio le opportunità che esso offre. In tal senso, sorprende l'attualità del plautino adagio "*homo homini lupus*".

Il padre dell'informatica giuridica , Vittorio Frosini[2], già nel lontano 1981, annotava: «*come la rivoluzione industriale moltiplicò l'energia fisica dell'uomo e ne diminuì la fatica, abituando l'uomo a convivere con le macchine* [...] *così la rivoluzione informatica allarga e potenzia le capacità della mente umana, obbligando la nostra intelligenza ad avvalersi di una protesi intellettuale*».

L'ecumene cibernetico, reso possibile da 'macchine' che riducono una mole impensabile di informazioni e dati in uno sciame di impulsi magnetici, non solo

1 Cit. Macrobio, Saturnalia, I, 9, 11: «*il mondo va sempre, muovendosi in cerchio e partendo da sé stesso a sé stesso ritorna*».

2 FELLUGA G.: *I Computer Crimes: definizioni ed elementi principali*, in *Tigor, Rivista di scienze della comunicazione*, n. 1, 2012, 27.

consente a ciascuno di essere ovunque ed in nessun luogo, ma permea di sé settori nevralgici: da quello militare a quello bancario, dalle attività economiche e scientifiche a quelle delle Pubbliche Amministrazioni.

L'uso massivo dei prodotti e della tecnologia informatica, che trovano nel *web* l'*habitat* naturale, diventano il mezzo e/o l'oggetto di fatti criminosi nuovi. Le fattispecie tipiche, storicamente cristallizzate nella legge penale, pressate dall'incessante evoluzione tecnologica, mostrano inesorabilmente le proprie lacune di fronte all'eterogeneità delle modalità dell'offesa, dell'oggetto su cui essa ricade e del ruolo assunto dal *computer*. G. Faggioli[3] - nel 1998 - osservava: «*La difficoltà di definire il concetto di crimine informatico si pone in tutta la sua evidenza se si osserva che, né a livello di legislazioni nazionali, né in ambito internazionale è stato possibile elaborare una definizione unitaria »,* mentre G. Pomante - nel 1999 - *: « Individuare e definire compiutamente il fenomeno dei computer crimes è, obiettivamente, un compito arduo e complesso*»[4]; infine, R. Borruso – nel 2009 - fornisce un'immagine efficace, preziosa ed attuale: «*Un computer è un complesso unitario di macchine diverse per funzione, dotato di una straordinaria capacità di memorizzare qualsiasi tipo di dato e, quindi, d'incorporare il pensiero, passato o presente, con essi espresso, d'instancabile capacità d'operare a velocità vertiginosa calcoli, confronti, ricerche ed altre elaborazioni di vario tipo secondo l'algoritmo posto a base del programma, in grado di comunicare - trasmettendo e ricevendo - con tanti utenti diversi, ognuno singolarmente trattato, anche se sparsi nelle più lontane parti del mondo, complesso unitario cui l'uomo, proiettando nel futuro la sua volontà e le sue scelte, può dare tutt'insieme, attraverso un programma, una grandissima quantità di ordini mediati nel tempo, integrabili tra loro e condizionati, cioè subordinati ad eventi futuri ed incerti che è lasciato al computer stesso d'accertare, ordini che possono diventare, così, veri e propri criteri di giudizio e di comportamento, fino al punto da renderlo autosufficiente nell'espletamento di attività di vario genere, semplicemente informative o anche decisionali, interagenti con realtà dinamiche o comunque complesse, che per dimensioni e quantità di variabili,*

3 Cfr FELLUGA G., cit., 30.
4 Cfr FELLUGA G., cit., 29.

fuoriescono dalla possibilità di un controllo diretto umano e, quindi, fino al punto di farlo diventare una vera e propria intelligenza cd. "artificiale" operativamente superiore talvolta alle stesse facoltà dell'uomo che l'ha creata» [5].

Il *Cyberspace*, in realtà, muta le tradizionali categorie del "penale", dove il fatto materiale trasforma la realtà 'esterna' ed incide sulle relazioni intersoggettive[6]. Lo spazio 'virtuale' prende il posto della realtà fisica, mentre l'intermediazione del sistema informatico o telematico ridisegna le categorie penalistiche della condotta e dell'evento, nonché la determinazione del t*empus* e del *locus commissi delicti* [7]. L'armamentario fornito al criminale dalla tecnologia elettronica è micidiale, ma non tecnologicamente diverso da quello usato per fini leciti. Sebbene il *vulnus* inferto non abbia la dirompenza della fisicità, nondimeno gli effetti si caratterizzano per l'offensività, rientrando, perciò, nel penalmente rilevante.

Il linguaggio informatico conia termini nuovi: *Malware, virus*, *Trojan Horse*, *Logic Bomb etc*.. Sono vocaboli, perfino poetici, che indicano programmi ordinari (*software*), in grado di infettare replicandosi (*Malware*) o di nascondersi all'interno di programmi utili (*Trojan Horse* o *Spyware*) eludendo il controllo dell'utente, e, per questo, dotati di potenziale offensività in ragione dei fini avuti di mira dal criminale.

Il legislatore, ma anche la dottrina e la giurisprudenza, sono chiamati a studiare, analizzare e definire questo complesso di nuovi beni, condotte e strumenti. La responsabilità, infatti, si colora diversamente a seconda che il fatto sia ad esempio frutto di un *virus*, in senso tecnico, o di un programma che opera nocivamente per un errore del programmatore.

Nel *Cyberspace*, luogo senza spazio in quanto globale, condotte ed eventi assumono una dimensione transnazionale, persino mondiale[8]. Quest'estensione,

---

5 Cfr. BORRUSO R., RUSSO S., TIBERI C., *L'informatica per il giurista dal bit a Internet*, 3^ ed., Giuffrè, Milano, 2009, 570 ss

6 V. PICOTTI L., *Responsabilità penali in Internet*, in PASCUZZI G. (a cura di), *Diritto e informatica: l'avvocato di fronte alle tecnologie digitali*, Milano, Giuffré, 2002, 115-146; ID, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *il diritto penale dell'informatica all'epoca di Internet*, Cedam, Padova 2004, 21-94.

7 V. PICOTTI L., *Responsabilità penali*, cit., 175 ss.

8 V. PICOTTI L., *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. Trim. di dir. Pen. dell'econ*., n. 4 , 2011 , 827-864

peculiarità di fondo dei *Cybercrime*, ha reso urgente ed improcrastinabile il ravvicinamento della legislazione penale degli Stati che, tanto a livello europeo quanto extra-europeo, si è inverata con gli strumenti di armonizzazione[9]. Tra questi, paradigmatici sono la Convenzione *Cybercrime* del Consiglio d'Europa, le decisioni quadro, prima, e le direttive, poi, dell'Unione Europea. Le infrastrutture tecnologiche (reti, banche-dati) si caratterizzano infatti sempre più come elementi critici nelle economie di tutti gli Stati, perciò necessitano di una tutela efficace. L'incessante velocità dell'evoluzione e diffusione delle tecnologie informatiche rischia, invero, di vanificare gli sforzi di un legislatore, che, costretto in una sorta di competizione, spesso subisce l'azzardo di tradurre nel diritto positivo disposizioni inadeguate. Innanzi ad una, persino ridondante, produzione legislativa ci si può porre l'interrogativo se, nell'ordito del sistema penale, siano configurabili degli effettivi vuoti di tutela o se già esistano disposizioni adattabili ai nuovi illeciti.

L'intervento del nostro legislatore, invero, non sempre si è contraddistinto per una prospettiva d'insieme nel momento in cui ha introdotto le nuove fattispecie incriminatrici nel *corpus* del diritto penale[10]. Alla luce dell'intero sistema penale, a volte, egli pare dimenticare i princìpi primi che lo governano, primo tra tutti quello di offensività, nonchè di tassatività e di proporzionalità della pena[11]. Innegabilmente, tra le ragioni profonde di tali difficoltà, vi è il fatto che i nuovi "oggetti" informatici non sempre abbiano un substrato fisico tangibile, ossia non corrispondano pienamente alla "cosa" tradizionalmente intesa[12].

I mezzi ed i modi di realizzazione della condotta, poi, si connotano diversamente, rispetto alla concezione tradizionale dell'agire, in quanto sfruttano e si avvalgono delle nuove opportunità fornite dalla tecnologia informatica. Si suole

---

9 V. PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Diritto dell'Internet*, n. 2/ 2005, 189-204.

10 V. PICOTTI L., *Sistematica*, cit., 21 ss.

11 Su questi fondamentali tali principi penalistici v. BRICOLA F., *Teoria generale del reato*, in *Nov. Dig. It.*, vol. XIX, Utet, Torino 1973; ID., *Teoria generale del reato*, in *Scritti di diritto penale*, vol.I/I, Milano, 1997; MARINUCCI G., DOLCINI E., *Corso di diritto penale*, vol. I, II^ ed. Giuffrè, Milano, 1999; DONINI M., *Teoria del reato*, in *Dig. Disc. Pen.*,vol. XIV, Torino, 1999; VASSALLI G., (a cura di), *Problemi generali di diritto penale*, Giuffrè, 1982.; MANZINI V., *Trattato di diritto penale italiano*, agg. da Nuvolone e Pisapia, Utet, Torino, 1986. .

12 Sui danneggiamenti e la nozione di cosa-dato informatico, v. PECORELLA C., *Il diritto penale dell'informatica*, (cur. Picotti L.), Cedam, Padova, 2006, 61-81.

parlare di *Cybercrimes*[13], locuzione ormai invalsa nell'ambiente giuridico internazionale[14], valida non solo per contrassegnare la nuova tipologia dei fatti illeciti, ma anche per indicare il punto d'approdo nello sviluppo storico della normativa penale italiana. Il legislatore italiano, sollecitato, all'inizio, dalla necessità di far fronte ai primi attentati e sabotaggi ad impianti e centri di elaborazione dati[15], ed in seguito dall'impulso, dapprima internazionale (Consiglio d'Europa) e poi europeo (Decisioni quadro), conoscerà il passaggio dal concetto di C*omputer crime*[16] a quello di C*ybercrime*, quasi a significare l'acquisita consapevolezza circa la natura dei nuovi "oggetti "e delle nuove modalità di offesa, che sempre più frequentemente si realizzano mediante le reti telematiche ed in particolare in *Internet*[17].

Il tema della «*sicurezza informatica*» e della necessità di fornire una adeguata tutela in caso di una sua lesione, tradotta in svariate disposizioni nell'ordinamento, è materia di sicura attualità per il legislatore domestico. L'acerba fattispecie del danneggiamento informatico, introdotta dalla L. 547/93 con l'art. 635-*bis*, ha subìto una profonda revisione ad opera della legge 48/2008 di ratifica ed esecuzione della già menzionata Convenzione *Cybercrime*. La legge menzionata ha introdotto la bipartizione tra il danneggiamento di informazioni, dati e programmi elettronici (art. 635-*bis c.p.,* 635-*ter c.p.*) da un lato, e dall'altro dei sistemi informatici e telematici (art. 635-*quater* c.p., art. 635-*quinquies* c.p.); fattispecie che si sono affiancate a quelle prodromiche dell'accesso abusivo al

13 Sulla nozione di criminalità informatica, vedasi PICOTTI L., *Biens juridiques protégés et technique de formulation des infractions en droit pènal*, in *Revue International de droit pènal*, vol. 77, n.3/4, 2006, 525 ss.

14 V. ad esempio la Convenzione *Cybercrime* del Consiglio d'Europa.

15 La Legge 191/78 di contrasto al terrorismo politico riformulerà l'art. 420 c.p. «*Attentato ad impianti di pubblica utilità*».

16 Fra le molte fonti in tema di criminalità da *computer*: PICOTTI L., *Biens juridiques protégés*, cit., 525 ss.; SARZANA C., *Informatica, internet e diritto penale*, III^ ed., Giuffrè, Milano, 2010; SIEBER U., *Les crimes informatique e d'autres crimes dans le domaine de la tecnologie informatique, comentaire e questions préparatoire por le colloque de l'A.I.D.P. a Wüzbourg*, in *Riv. Int. de droit penal, colloque préparatoire*, Section 1, WÜRZBURG (Germania) – Würzbourg, 5-8 octobre 1992, A.I.D.P., Érés, Vol. 64, 1° e 2° trimestres 1993. 64), 1993; AIDP, XV^{eme}CONGRÈS INTERNATIONAL DE DROIT PENAL, Rio de Janeiro, 4-10 septembre 1994, *Résolutions*, *Section* II, *Infractions informatique e autres crimes contre la tecnologie informatique*, in *R.I.D.P.P.*, 66^{e} année, 1^{e} e 2^{e} trimestres, 1995, 27-35.

17 Il cosiddetto *Cybercrime* in 'senso stretto' indica una tipologia di reati che possono essere commessi solo nel cd. *Cyberspace* tramite le *reti* telematiche. Per approfondimenti sul tema vedasi PICOTTI L., *Biens juridiques protégés*, cit., 525 ss.

sistema informativo (art. 615-*ter* c.p.), della detenzione e diffusione abusiva di codici di accesso (*art.* 615-*quater* c.p.) nonché della diffusione di apparecchiature, dispositivi o programmi diretti a danneggiare o interrompere un sistema elettronico (art. 615-*quinquies* c.p.).

L'attualità della materia «*sicurezza informatica*», in particolare dei «*danneggiamenti informatici*», è testimoniata dallo sforzo nell'allineare la normativa interna dapprima alle raccomandazioni del Consiglio d'Europa (R(89) e, poi, alla Convenzione *Cybercrime*, nonchè alle iniziative europee, prima tra tutte, la Decisione Quadro 2005/222/GAI sugli attacchi ai sistemi di informazione, ed oggi la Direttiva 2013/40/UE.

Tuttavia, come già anticipato, l'urgenza di provvedere a colmare le lacune normative, già sottolineate da attenta dottrina[18] nonchè dalla stessa giurisprudenza, è andata spesso a discapito della qualità tecnica e sistematica. Il risultato è consacrato in una farraginosa normativa interna che non pare garantire, in senso pieno, il raggiungimento di quell'armonizzazione e rafforzamento della cooperazione internazionale tra gli Stati, ragione ultima avuta di mira dagli strumenti internazionali [19]. Un tema come il nostro, proprio per la sua intrinseca vocazione alla extraterritorialità, impone la doverosità di un' indagine di diritto penale comparato, avendo di mira quel che successe e succede negli ordinamenti penali degli altri Stati europei, in particolare quelli che appartengono ai sistemi di *civil law*.

Orbene, negli anni Novanta, sia il legislatore tedesco (con la 2. WiKG [20]) che quello italiano[21] introdussero nei rispettivi ordinamenti penali le prime fattispecie incriminatrici autonome, per punire gli attacchi commessi a danno o mediante le tecnologie dell'informazione[22].

---

18 V. , per tutti, gli svariati contributi di PICOTTI L., SARZANA C., PECORELLA C., BORRUSO R. CORASANITI G., D'AIETTI G., PASCUZZI G., PICA G..

19 Cfr. L. PICOTTI, *Profili di diritto penale e sostanziale*, in *Dir. pen. e proc*., n.6, 2008, 716.

20 *Zweit Gesetz zur Bekämpfung der Wirtschaftskriminalität* (2.WiKG), 15 maggio 1986, pubblicata nel *Bundesgesetzball*, n. 21 del 23 maggio 1986 (BGBI 1986,I,721). Per un commento ed esaustivi riferimenti bibliografici vedasi PICOTTI L., *Diritto penale dell'informatica*, cit., 21-94.

21 L. n. 547/93 del 23 dicembre 1993.

22 In particolare: gli accessi abusivi, le intercettazioni di dati, i danneggiamenti elettronici e la frode informatica

Diversamente si atteggiò quello spagnolo[23], che scelse, invece, di estendere esclusivamente l'ambito applicativo dei reati tradizionali (ad es. danneggiamento di cose e truffa). Ciò fece, seguendo il metodo dell'estensione analogica delle fattispecie tradizionali ai nuovi fatti criminosi, qualora commessi con l'ausilio delle nuove tecnologie. La metodologia utilizzata ai fini dell'ampliamento, da un lato, teneva conto delle nuove modalità commissive creando delle sottofattispecie autonome rispetto a quelle tradizionali, dall'altro ampliava l'oggetto materiale di quei delitti che presentavano analogie con le nuove fattispecie criminose[24].

Solo con la riforma del 2010, il legislatore iberico [25] ha introdotto nuove ed autonome fattispecie delittuose in materia di danneggiamento informatico nel *corpus* del *Código Penal* (artt. 264.1 CP spag. e 264.2 CP spag.) e, per il resto, ha confermato la tecnica legislativa adottata nel 1995. Con la novella, in realtà, egli ha cercato di far proprie le prescrizioni della Decisione Quadro 2005/222/GAI sugli attacchi ai sistemi di informazione e danneggiamento dei dati informatici ed in parte quelle della Convenzione *Cybercrime* del Consiglio d'Europa.

La ricezione di tali fonti ha prodotto un allineamento dell'ordinamento penale spagnolo agli altri ordinamenti continentali, in particolare quello italiano, sebbene permangano degli aspetti di criticità.

Le assonanze ed i distinguo tra la normativa italiana e quella spagnola, pertanto, rendono particolarmente interessante uno studio comparativo volto ad evidenziare gli aspetti di maggiore criticità e relativi alle scelte di politica criminale, alle modalità d'adeguamento della legislazione penale domestica agli obblighi di fonte sovranazionale, alle tecniche di formulazione del fatto tipico, alla collocazione sistematica delle fattispecie, nonché al rispetto o meno del principio di proporzionalità nella determinazione delle sanzioni.

Come si vedrá meglio in seguito, il legislatore iberico, ma non è il solo, ha perso l'occasione di dare piena attuazione ad alcune importanti prescrizioni della Convenzione *Cybercrime*, limitando il proprio intervento all'attuazione della

23 Cfr. Ley Organica n. 10 del 23 novembre 1995

24 Per un commento sull'operato del legislatore iberico v. SALVADORI I., *I nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica n. 5/10. Profili di diritto comparato*, in *L'indice penale*, anno XIV, n.2, 2011, pag. 767-794.

25 Cfr. Ley Organica n°5/2010 - pubblicata sul *Boletín Oficial del Estado* il 23 giugno 2010 ed entrata in vigore il 22 dicembre 2010.

Decisione Quadro 2005/222/GAI. In tal modo risulta ancora incompiuto l'auspicabile processo di armonizzazione legislativa tra gli Stati, presupposto imprescindibile per l'efficace ed omogeneo contrasto a livello europeo della criminalità informatica, come richiesto anche dall'art. 83 T.F.U.E..

Capitolo I

LINEE STORICO – EVOLUTIVE: DAI *COMPUTER CRIMES* AI *CYBERCRIMES*

SOMMARIO:

1. La ricerca di una definizione di bene informatico: una breve indagine storica sull'impossibilità di raggiungere l'obiettivo di qualificare il *Computer crime* con un concetto unitario.
2. L'atteggiamento del legislatore italiano degli anni Novanta: definizione dei *Computer crimes*. Brevi cenni alla tecnica di formulazione legislativa.
3. Il *Cybercrime*: verso una nuova dimensione e concezione di bene giuridico protetto.
4. Nuove problematiche dal *Cyberspace*: cenni alle questioni di giurisdizione correlate al *Cloud computing*.

1. *La ricerca di una definizione di bene informatico: una breve indagine storica sull'impossibilità di raggiungere l'obiettivo di qualificare il Computer crime con un concetto unitario.*

Mettendomi di buona lena alla ricerca del significato dell'aggettivo 'informatico' mi sono concessa l'azzardo di avvalermi del più 'laico' dei libri a disposizione: un vocabolario[26].

"Informatico", secondo *Lo Zingarelli*, significa: «*relativo all'informatica*». Prendo atto del rinvio e leggo la pertinente definizione: «*[dal francese informatique, composto da inform(ation electronique ou automati)que, 1968]. Scienza e tecnica dell'elaborazione di dati e, generalmente, del trattamento automatico delle informazioni*». Mi sorprende la freschezza neologica di un temine oggi tanto familiare, anche per chi non sia nativo digitale. Lasciate alle spalle queste svagate suggestioni, riprendo la linea maestra dell'indagine scientifica sul tema in argomento.

Orbene, l'uso illecito delle nuove tecnologie dell'informazione e la necessaria reazione sul piano giuridico rappresentarono (e rappresentano) un intreccio di cruciale importanza sul quale si sono appuntate sia l'attenzione sia l'opera del legislatore nazionale. L'analisi storiografica, strumento indefettibile per comprendere i fatti umani e via maestra per indagarne i percorsi concettuali e/o

26 V. ZINGARELLI N., *Lo Zingarelli*, ed. 2012, voci: informatico e informatica, 1138.

culturali, consente di dar conto, in modo stringente, di quali siano stati (e sono) i problemi d'inquadramento sistematico e dogmatico delle nuove figure d'illecito, di compiere un bilancio sull'efficacia degli interventi normativi e di tracciarne l'ipotetica linea evolutiva.

La traduzione nel diritto positivo di norme nuove o il riadattamento di quelle previgenti, incalzate dall'eterogeneità delle condotte illecite, prospettano e presumono anzitutto la soluzione di problemi definitori. Tra essi, un ruolo centrale viene occupato tanto dalla nozione di *bene giuridico tutelato*[27] quanto dall'indagine sulla portata e i limiti del nuovo concetto di *Computer crime*. Tramite la luce riflessa dalla storia, si può cogliere, poi, quel passaggio culturale e concettuale dall'anzidetta nozione a quella di *Cyber crime*.

Orbene, dal punto di vista strettamente storico, gli anni Sessanta rappresentarono il punto d'inizio del fenomeno d'informatizzazione globale. Grazie al *transistor*, comparvero le prime macchine di calcolo, che da subito ebbero un'importante diffusione nelle imprese e pubbliche amministrazioni. Le ragioni di tal successo riposavano nel basso costo e nelle dimensioni degli elaboratori, già particolarmente contenute. Questi, in estrema sintesi, furono i fattori fondanti il successo e l'esponenziale incremento nell'uso della tecnologia informatica. I *computer*, prima degli anni Settanta, erano dei semplici *terminali* che consentivano l'accesso ad un *computer* centrale, il *Mainframe*, ma solamente quest'ultimo era dotato delle capacità computative e di elaborazione dei dati digitalizzati. I delitti perpetrati contro tali beni furono, per lo più, di natura fisica, ossia in danno al sistema informatico (*hardware*) e, solo di riflesso, ai dati in esso immagazzinati. Paradigmatico l'aneddoto dell'incendio che causò la distruzione del *data-base* di un'università canadese in occasione di una rivolta studentesca. Negli USA, per altro verso, si fece largo l'idea di creare delle banche-dati per tutti i Ministeri, ma, al contempo, ci si preoccupò di garantirne l'adeguata protezione giuridica, anche dal punto di vista di tutela della riservatezza (o *privacy)*, nonché dell'integrità e disponibilità dei dati e dei sistemi stessi.

Negli anni Settanta, l'ulteriore caduta di prezzo dei *terminali* e dei *Mainframe* funse da voláno all'ulteriore diffusione della tecnologia

27 Cfr. ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico*, Giuffrè, Milano, 1983, 3 ss.

dell'informatica. Contraltare al fenomeno fu l'incremento di nuove forme di delinquenza. Pur se i danni fisici ai sistemi elettronici continuavano ad essere la forma più importante di aggressione, apparvero nuove tipologie di delitti, genericamente definiti *informatici*. Tra essi, l'utilizzazione illecita dei sistemi informatici e l'alterazione dei dati elettronici. La transizione, poi, da forme di scambio manuale di denaro a quelle effettuate con sistemi elettronici occasionò, ad esempio, nuove e sofisticate forme di truffa o meglio di frode informatica, commesse mediante le nuove tecnologie. Anche in Italia il fenomeno si presentò nelle condotte abusive del prelevamento di contante dagli sportelli *bancomat*[28], in quelle fraudolente in danno ai sistemi informatici di gestione contabile di aziende ed istituti bancari, nei sabotaggi di centri di elaborazione dati[29]. In quel periodo la latitanza di una normativa penale *ad hoc* costringeva la giurisprudenza italiana ad arguzie interpretative ed i nuovi fenomeni vennero convogliati, a volte forzatamente, nell'alveo del penalmente conosciuto, mentre il legislatore apprestava norme dal connotato emergenziale e si imposero, con forza, i problemi definitori[30].

Le svariate forme di abuso degli elaboratori elettronici ed il connesso problema della loro rilevanza penale, infatti, non potevano esimere dall'indagine sulla portata e sui limiti del concetto di *Computer crime*. A tale ultima espressione, coniata dalla dottrina nordamericana, si contrappose, ben presto, quella di *computer related crime*: occorreva sottolineare che il *computer* non è l'autore del reato, bensì lo strumento di cui l'autore s'avvale per commetterlo[31]. In sostanza, a fondamento del concetto si assunse l'esistenza di un collegamento tra la condotta e l'elaboratore elettronico. Se il minimo comun denominatore era, dunque, il carattere informatico dell'illecito, era pur vero che esistevano illeciti, come l'uso abusivo di carte magnetiche di pagamento, che non presupponevano alcuna

28 V . Art. 12 della legge 5.7.1991, n. 197.

29 V. L. 191/78 adottata in seguito all'attacco in danno della banca-dati motorizzazione civile da parte delle brigate rosse.

30 Sulle prime forme di danneggiamento informatico cfr. PICOTTI L., *Criminalità da computer e diritto penale dell'informatica*, in *Studi di diritto penale dell'informatica*, Verona, 1992; ID, *Commento alla sentenza del tribunale di Firenze*, 27 gennaio 1986, in *Dir. Inf. Inf.*, 1986, 962 ss; ID, *La rilevanza penale degli atti di 'sabotaggio' ad impianti di elaborazione dati*, in *Dir. inf. inf.*, 1986, 969 ss.

31 Sul punto vedasi PARKER D.B., *Crime by computer*, New York, 1976, USA .

conoscenza tecnologica[32], benché si parlasse di *Computer crime*; ne conseguì che lo sforzo di costruire una categoria unitaria di *Computer crime* risultò inane. Le stringate considerazioni svolte, in realtà, chiariscono le difficoltà che si riscontrarono nella dottrina penalistica agli albori degli anni Settanta, allorquando si manifestarono le prime forme di criminalità nel settore informatico. L'idea di poter costruire un concetto unitario di *Computer crime* richiedeva non solo di isolare gli elementi di peculiarità della condotta e dell'oggetto, ma soprattutto, di ascrivere in quella nozione qualsiasi fatto illecito che presentasse quelle caratteristiche. L'eterogeneità delle manifestazioni abusive, in realtà, era priva di un qualsiasi valore euristico e delimitativo. Il citato collegamento con l'elaboratore poteva essere del tutto casuale e, di conseguenza, poteva rendere ingiustificata, sotto il profilo penale, una diversa considerazione della condotta: la sottrazione di un *floppy disc* era (e rimaneva) pur sempre un furto *ex* art. 624 c.p.. La migliore dottrina tentò di circoscrivere l'ambito dei *Computer crime* a fatti nei quali «*il computer è l'oggetto o lo strumento dell'azione*»[33]. Orbene, in tale definizione non erano distinguibili, in modo chiaro, le forme di aggressione alle componenti *fisiche* del sistema informatico rispetto a quelle *logiche* e, per questa via, l'epilogo non avrebbe goduto di miglior sorte. Taluno prospettò pure una definizione che operasse la distinzione tra condotte che avessero ad oggetto la componente materiale (*hardware*) e quelle derivanti dall'uso della tecnologia elettronica, che comunque presupponeva la preliminare classificazione delle condotte abusive. L'impiego di un'ampia nozione di *Computer crime*, peraltro adottata anche presso gli organismi internazionali[34], allargando le maglie del concetto in argomento si poneva in discrasia col criterio di individuazione, estremamente selettivo, delle condotte passibili di considerazione penale. Il ceppo originario della criminalità informatica fu ravvisato specialmente in una serie di aggressioni al patrimonio e ricondotto a diverse forme di manipolazione dei dati, come l'impiego fraudolento

32 U.S. DEPARTEMENT OF JUSTICE, NATIONAL CRIMINAL JUSTICE INFORMATION AND STATISTIC SERVICE, *Computer crime: Criminal Justice Resouce Manual*, WASHINGTON, 1979.

33 Cfr. LENCKNER T., *Computer-kriminalität und Vermögensdelikte*, Karlshrue, 1981, 13 ss., secondo cui l'agente dovrebbe sfruttare per i propri fini le specialità tecniche del processo di elaborazione elettronica.

34 Cfr. CONSEIL DE L'EUROPE, *La criminalité des affaires, Recomandation n° R(81) 12*, Stasbourg, 1981; PARKER D.B., *Crime by computer*, New York, 1976, USA .

dell'elaboratore, il sabotaggio informatico ed il danneggiamento di dati e programmi, lo spionaggio informatico o l'indebita acquisizione di dati ed informazioni contenute nell'elaboratore, e il furto di tempo, ossia l'uso non autorizzato del tempo d'elaborazione di un sistema elettronico [35]. Si trattava di accezioni di «reato informatico» restrittive e condizionate da un concetto di criminalità informatica fortemente legato all'ambito economico e degli affari[36].

Negli anni Ottanta si fece poi largo l'idea di spostare le operazioni di calcolo nei singoli *terminali* e comparvero i *personal computer*, macchine dotate di una maggiore potenza elaborativa e che permettevano di avere fogli di calcolo (*xls*) ed un *editor* di testi (*word*). Quegli anni, in realtà, segnarono il punto di non ritorno del processo di globalizzazione digitale, grazie alla diffusione capillare dei *personal computer*. Per contro, un tale fenomeno andò ad incrementare i possibili obiettivi di attacco, primi tra tutti, quelli ai sistemi informatici di un'ampia gamma di infrastrutture critiche essenziali. L'aumento, la prolificazione e l'importanza dei programmi per elaboratori (*software*) determinarono, al contempo, le prime forme di pirateria elettronica e dei delitti correlati alla tutela della paternità delle licenze d'uso.

L'ampia interconnessione, grazie alla diffusione delle reti *web*, offrì al delinquente la possibilità di entrare nei sistemi informatici consentendogli di non essere presente nel luogo del delitto. Peraltro, la possibilità di distribuire *software* tramite il *download* dalla rete permise ai criminali di diffondere *software* maligni (*Malware*) e si assistette all'aumento nel numero di *virus* informatici.

Al vuoto di tutela legislativa, che spesso rendeva inane la risposta penale di molti Stati, si contrappose il fervore degli studi e delle ricerche, spesso di respiro sovrannazionale. Il fine perseguito dagli svariati organismi consistette nello studio di risposte efficaci, anche di natura legislativa, per porre argine alle *nuove forme di aggressione* a beni della vita tradizionali ed offrire una tutela efficace a *beni totalmente nuovi* (ad es. riservatezza e sicurezza informatiche). Iniziò,

35 Cfr. C.PECORELLA, *Diritto penale dell'informatica*, II^ ed., Cedam, Padova, 2006, 3 ss.

36 Cfr. TIEDEMANN K., *Wirtschaftsstrafrecht und Wirtschaftkriminalität*, Reinbeckbei Hamburg, 1976; KAISER G., *Criminologi*a, trad. it. a cura di Morselli e B. Blonk Steiner, Milano 1985; prospettiva iniziale seguita anche dal CONSEIL DE L'EUROPE; si giunge a restringerne l'ambito ai soli comportamenti offensivi di interessi economici e patrimoniali, così SIEBER U., *Computerkriminalität und Strafrecht*, Köln, 1977, 2^ ed. 1980.

dunque, il processo di attualizzazione delle legislazioni, per operarne l'adattamento al nuovo ed evolutivo contesto della delinquenza. A un tale processo non poteva difettare l'apporto delle organizzazioni internazionali, anche sotto il profilo di un contributo nella definizione di una tipologia unitaria di *Computer crime*. L'O.C.D.E. (*Organisation for Economic Cooperation and Development*) ed il Consiglio d'Europa crearono commissioni di studio per analizzare il fenomeno e valutare le possibili risposte giuridiche. A livello sovrannazionale, O.N.U. e O.C.D.E. si occuparono della criminalità telematica nell'ambito di consessi internazionali, quali il *Global Business Dialogue* e il *Trans-Atlantic Business Dialogue*. Nel 1983 l'O.C.S.E. condusse uno studio sulla possibilità di applicare, secondo una prospettiva di armonizzazione, le leggi del diritto penale, onde assicurarne l'incisività per la lotta contro il crimine informatico.

Nell'incontro, tenutosi a Parigi nel 1983, si definì *Computer crimes*: «*ogni condotta antigiuridica, disonesta o non autorizzata concernente l'elaborazione automatica e /o la trasmissione dei dati, comprendendo pertanto in tale nozione anche le violazioni della privacy*». Risale al 1986 lo studio "*Computer-Related Crime: Analysis of Legal Policy*" nel quale, effettuata un'analisi delle leggi esistenti e delle proposte di riforma presentate da alcuni Stati membri, gli esperti dell'O.C.D.E. raccomandavano la necessità di perseguire penalmente alcuni abusi testualmente elencati. L'enumerazione delle nuove manifestazioni della criminalità informatica, pur funzionale all'esigenza di dare indicazioni e raccomandazioni ai legislatori nazionali, in realtà è una prassi che andrebbe accolta solo se sia in grado di fissare i connotati di *specificità* della categoria *Computer crime*. Aspetto, quest'ultimo, assai importante pur se non riguarda esclusivamente il modo o il mezzo tecnico di realizzazione del fatto illecito. Detto diversamente, le condotte prese in considerazione avrebbero dovuto presentare dei tratti di novità che giustificassero apposite previsioni normative o autonome soluzioni interpretative, applicative, scientifiche e dottrinali[37].

La Raccomandazione 9 (89) del 13 settembre 1989 «*sur la criminalité en relation avec l'ordinateur*» da parte del Comitato dei Ministri del Consiglio

37 Cfr PICOTTI L., voce *Reati informatici*, in *Enc. Treccani*, 2000, 2 ss.

d'Europa segnò il punto di svolta nella ricerca di una definizione "ordinaria" di criminalità informatica e delle disquisizioni in ordine alla comprensione, o meno, delle condotte nel suo alveo. Venne, di fatto, abbandonato ogni tentativo di ricostruzione unitaria del concetto, a favore di una descrizione delle singole condotte abusive che gli Stati erano invitati a punire con una sanzione penale. Rinviando l'approfondimento sui contenuti di tale strumento, basti dire che le condotte di abuso dell'informatica vennero suddivise, dagli esperti del Consiglio d'Europa, in due gruppi (lista minima e facoltativa.)[38]. Gli Stati erano chiamati a reprimere penalmente solo le condotte previste nella lista minima, anche ricorrendo ad interventi legislativi *ad hoc*, mentre, per quelle indicate nella facoltativa, la scelta era rimessa alla loro insindacabile valutazione. In definitiva, la nozione di *Computer crime* si mostrava priva di uno stringente significato tecnico-giuridico, quindi inutilizzabile per focalizzare da sola gli aspetti salienti della disciplina sanzionatoria e precettiva delle condotte di abuso dell'informatica.

2. *L'atteggiamento del legislatore italiano degli anni Novanta: definizione dei Computer crimes. Brevi cenni alla tecnica di formulazione legislativa.*

Il legislatore "domestico", posto di fronte ad oggetti e condotte rapportabili alle nuove tecnologie, ebbe due alternative: non introdurre fattispecie nuove, laddove ritenesse sufficiente ampliare l'oggetto delle disposizioni vigenti, oppure creare norme totalmente nuove di portata generale o speciale. In quest'ultima ipotesi avrebbe dovuto fornire la puntuale descrizione del tipo d'illecito informatico, nonché la definizione degli elementi e delle condizioni espressamente qualificate dalle nuove tecnologie.

La differenziazione in argomento, contrariamente all'ovvia deduzione, non è tuttavia così netta.

Nel primo caso l'operazione, in sostanza, si sarebbe tradotta in un *restyling* definitorio di precedenti incriminazioni, lasciandone inalterata sia la struttura sia la formulazione, introducendo elementi (oggetti, mezzi, modalità della condotta)

38 Sul punto cfr. PECORELLA C., *Il diritto penale dell'informatica*, cit., 1-28.

che implicassero l'uso o l'applicazione della tecnologia informatica. Tale tecnica, in sé, aveva il vantaggio di non riscrivere *ex novo* le incriminazioni, garantendo apparentemente una maggior continuità nell'interpretazione ed applicazione del diritto. Si accettava, al contempo, il rischio di non controllare gli effetti prodotti dalle innovazioni introdotte nel *corpus* del codice penale. In realtà, la simmetria fungeva da elemento di legittimazione delle nuove scelte punitive. Le peculiarità che ammantavano i *nuovi* oggetti passivi o la modalità della condotta, benché analoghi a quelli tradizionali, determinavano invero una singolare configurazione del *bene protetto*.

Il legislatore veniva colto in contropiede dall'effetto imprevisto della combinazione tra nuove e preesistenti definizioni ed il contraccolpo si dimostrò foriero di specifici problemi tecnici e di struttura, data l'incidenza sulla descrizione della condotta prevista dagli illeciti. Non va nascosto che una siffatta tecnica di formulazione legislativa dissimulava una certa ritrosia nell'abbandonare i modelli preesistenti, sebbene apparisse, in astratto, maggiormente rispettosa delle esigenze di legalità e precisione nella descrizione dell'incriminazione.

Le nuove previsioni erano una sorta di *aggiornamento tecnologico* d'incriminazioni preesistenti sotto il profilo della condotta, ma non cambiava l'interesse protetto: paradigmatica la formulazione dell'art. 635-*bis* c.p. «*danneggiamento di dati e sistemi informatici*» proposta con la l. 547/93.

L'articolo in questione, strutturato e modellato in stretta analogia con il reato *comune* di danneggiamento di cose ex art. 635 c.p., tipizzava le condotte del «*distruggere, deteriorare, rendere in tutto o in parte inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui*». L'oggetto materiale sul quale potevano cadere le condotte riguardava, al contempo, cose materiali (*hardware*) ed altre totalmente immateriali (dati, programmi, informazioni). Nel trattamento ed elaborazione dei dati, in realtà, le condotte tipizzate dall'art. 635-*bis* c.p. non avevano né un significato di violenza né d'illiceità, essendo operazioni assolutamente consuete se non necessarie. Infatti, da un lato, il difetto di materialità rendeva impossibile l'individuazione del requisito intrinseco della «*violenza sulle cose*»; dall'altro, il concetto di *altruità*

rimandava alle nozioni extrapenali di *proprietà*, *possesso, uso* o *godimento* che affatto si attagliavano ai beni immateriali[39]. Infine, il paradigma dell'*inservibilità*, anch'esso correlato all'idea di un'integrità fisica, non coglieva l'importanza del *corretto svolgimento del programma* o delle sue *funzioni* od *utilità*.

Oggi, una maturata consapevolezza radica in questi ultimi concetti il presupposto logico della tutela avverso ogni forma di danneggiamento a dati e sistemi informatici, ancorandolo ai beni paradigmatici dell'*integrità* e della *sicurezza* informatica. L'articolo in questione, infatti, verrà riformulato dalla l. 48/08, che ha recepito le indicazioni contenute nella Convenzione *Cybercrime* di Budapest, pur se la sua formulazione rimane a tutt'oggi insoddisfacente.

La simmetria tra nuove e vecchie fattispecie è impressa anche nella struttura dell'art. 615-*ter* c.p. «*accesso illegale a sistema informatico e telematico*», fattispecie prodromica all'eventuale danneggiamento dei dati e sistemi elettronici. L'articolo in questione venne modellato sulla struttura dell'art. 614 c.p. «*violazione di domicilio*», del quale ripropose gli elementi materiali della condotta. La disposizione, in realtà, si riferiva ad un contesto ben diverso, virtuale e alternativo, dell'introduzione illegale o mantenimento nel sistema informatico o telematico contro la volontà del titolare dello *jus excludendi.*

L'analogia strutturale tra le nuove e preesistenti fattispecie, pur garantendo una familiarità di concetti, costringeva le prime entro schemi obsoleti. Una maggiore autonomia nella specificazione degli elementi costituitivi delle nuove incriminazioni non avrebbe determinato la lacerazione nella pregnanza e precisione delle stesse formule tradizionali: effetto, quest'ultimo, dovuto alla difficoltà di includere fatti, condotte ed oggetti profondamente diversi.

Gli esempi menzionati tratteggiano la fisionomia di un legislatore noncurante del rispetto del principio di tassatività, svagato nel selezionare sia il bene da tutelare, sia le specifiche modalità della sua aggressione. Egli dimentica che l'azione penale è degna solo se i predetti elementi siano delineati

39 Cfr. PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in PICOTTI L. (cur.), *il diritto penale dell'informatica nell'epoca di internet,* Cedam, Padova, 2004, 50-53.

rigorosamente; nel diritto penale le parole "pesano". Peraltro, con una siffatta tecnica di formulazione legislativa, il nostro legislatore non è riuscito a scongiurare il pericolo di persistenti lacune od inaccettabili superfetazioni. Il fatto non deve destare sorpresa o scalpore. La scelta tecnica del nostro legislatore di formulare le nuove fattispecie affiancandole alle preesistenti non fu una predilezione isolata, bensì condivisa da altri ordinamenti continentali come ad esempio quello spagnolo.

3. *Il Cybercrime: verso una dimensione e concezione nuove di bene giuridico protetto.*

Addentrarsi nel tema del «*danneggiamento informatico*» significa analizzare il diritto sostanziale e tracciare il quadro d'insieme della categoria identificando l'interesse protetto. Occorre, poi, collocare il fenomeno in argomento nel contesto giuridico-dogmatico per potervi riallacciare le problematiche definitorie in ordine alla nozione di *Computer/Cybercrime.*

Le funzioni assegnate al concetto di bene giuridico dalla teoria del reato, nel nostro campo, hanno un'operatività del tutto peculiare. Si tratta, qui, di valorizzare gli elementi comuni e differenziali delle singole fattispecie penali o loro insiemi omogenei per verificarne, poi, la corretta collocazione entro il quadro sistematico. Delineare questi aspetti significa, dunque, effettuare un'indagine storiografica, ma senza abbandonarsi alla semplice speculazione tautologica sulle disposizioni legislative introdotte nell'ordinamento. La dottrina penalistica, infatti, avvalendosi del procedimento euristico ed ermeneutico, è riuscita (forse) a dar conto dei modelli, delle fonti ispiratrici e della collocazione topografica dei nuovi illeciti introdotti nel diritto positivo. Tali speculazioni, abbandonata la pretesa di ridurre ad un'unità concettuale la nozione *Computer/Cybercrime*, hanno, sì, richiesto d'avere un parametro che fungesse da strumento d'indagine, ossia il bene giuridico tutelato, ma nella maturata consapevolezza della pluralità di funzioni che gli sono attribuite [40]. Orbene, fu chiaro allora che l'indagine dovesse avere una prospettiva strettamente deducibile dalla legislazione vigente. Quando la comparazione tra le

40 Cfr ANGIONI F., *Contenuto e funzioni*, cit., 3-242.

varie fattispecie penali fu letta alla luce di un'interpretazione evolutiva ed estensiva, salvo il divieto di interpretazione analogica, si comprese il senso della realtà positiva introdotta dalle nuove norme e, al contempo, si poterono suggerire al legislatore gli aggiustamenti o la creazione di ulteriori nuove norme.

Oggi, l'approccio di ordine empirico, quindi sostanziale, supera l'agognata idea di poter ricondurre il fenomeno *Computer crime* in un concetto unitario e di granitica consistenza e, al contempo, stimola la conoscenza e lo studio dei suoi profili tecnici, particolarmente utili ai fini delle inchieste e della raccolta delle prove. La descrizione fenomenologica dei reati informatici, infatti, dà contezza dei molti comportamenti meritori di una considerazione penale, pur se sorge il problema di identificare quali siano i beni giudici lesi, giacchè, in alcuni casi, è addirittura difficile cogliere il requisito dell'offensività: la mera detenzione di programmi dannosi o di codici d'accesso altrui, senza diffusione e comunicazione ad altri, sembrerebbe un comportamento innocuo.

L'illecito informatico, in fatto, "*bipolarizza*" la nozione di *infrazione* in due sottotipologie: *informatica* (*Computercrime*) e *cibernetica* (*Cybercrime*).

Il concetto di *infrazione informatica* tende ad assumere una connotazione elastica, grazie all'interpretazione estensiva ed evolutiva. Quest'ultima, a sua volta, è in grado di indurre una sorta di processo di adattamento del diritto positivo, necessario per far fronte all'incalzante evoluzione delle nuove tecnologie dell'informazione e della comunicazione. In altre parole, le fattispecie incriminatrici comuni, pur non presentando espressamente gli elementi tipici dell'informatica, possono essere aggiogate alla funzione di offrire tutela contro gli illeciti commessi con le nuove tecnologie. In particolare, il concetto di *infrazione informatica*[41], *stricto sensu* (*Computer crime*) si può adattare anche alle infrazioni riferibili alle procedure, mezzi, oggetti e prodotti propri della tecnologia dell'informazione e della comunicazione a distanza[42] e non concepibili al di fuori

41 Ossia quell'illecito in cui lo strumento informatico è il mezzo occasionale per la commissione del reato tradizionale.

42 A titolo esemplificativo: l'elaborazione *dati*, il loro trattamento o trasmissione, la realizzazione di programmi e la loro messa a disposizione o riproduzione tramite sistemi telematici, danni ai programmi e supporti informatici.

di quest'ultimo contesto. Le forme d'uso illecito delle nuove tecnologie[43] sono mutate rispetto agli anni Novanta ma, sebbene siano in costante evoluzione, si sono ridotte vieppiù ad un semplice stimolo per riformulare, riformare o modificare le norme vigenti, introdotte da riforme legislative, magari vaghe, ma comunque in grado di offrire una tutela penale.

Il concetto di *infrazione cibernetica* (*Cybercrime*) si caratterizza, invece, per la peculiarità dell'oggetto sul quale ricade l'azione criminosa: il *software* di un sistema informatico o di una *rete* di *computer*. Il *Cybercrime*, ai fini giuridici, diviene criterio identificativo delle nuove tecnologie informatiche qualificate dall'*automazione* nelle operazioni di trattamento, riproduzione e trasmissione dei *dati* sotto forma elettronica. *L'automazione* necessita di appositi *software* in grado di 'processare' o 'trattare' un'*informazione*, intesa in senso generico. Quest'ultima, in realtà, può essere tanto l'oggetto di interventi manuali da parte dell'uomo, quanto della menzionata procedura informatica. In quest'ultimo caso l'accezione di *informazione* si attaglia a dati non leggibili né destinati all'uomo, giacché destinati al sistema informatico o relativi al suo funzionamento interno. Il carattere informatizzato/automatizzato, tramite *software* specifici, delle operazioni di trasmissione e trattamento dei dati, nuova caratteristica dell'informatica, permette la sostituzione parziale o totale delle attività concretamente svolte dall'uomo. Un tal fatto incide sul contenuto cognitivo e/o decisionale ed è una caratteristica significativa, sul piano giuridico e penale, nella misura in cui influenza la struttura della condotta o la qualità dei mezzi implicati nella commissione del reato[44]. L'epoca digitalica con le sue implicazioni in chiaroscuro e la riprovazione serbata dal legislatore avverso le sue distorsioni hanno consacrato questa nuova categoria di reato definito cibernetico o *Cybercrime*. La nozione di *Cybercrime* vale ad identificare quell'illecito che si concretizza nella o per tramite della *rete*. Si tratta di una categoria *aperta*, anch'essa in grado di includere, oltre alle fattispecie che espressamente prevedano

43 E' ormai anacronistico il concetto di «*comportamenti socialmente dannosi considerati meritevoli di sanzione penale*» proprio della cd. teoria «*sostanzialistica*» secondo la quale il reato è un «*fatto socialmente pericoloso*» di per sé. Cfr. D'ARMA S., *Offensività e legalità: una discutibile soluzione in materia di violazioni urbanistiche,* in *Giur. Merito,* 1999, 106.

44 Cfr. PICOTTI L., *Biens juridiques protégés*, cit., 527 ss.

nei loro elementi costitutivi mezzi od oggetti informatici, anche beni giuridici tradizionali, qualora lesi con l'intermediazione dei nuovi mezzi di comunicazione telematica[45].

Una sommaria disamina sulla tecnica normativa prescelta dal nostro legislatore, consente di cogliere l'evidente partizione tra diverse categorie di reati elettronici in ragione del contenuto dei *beni giudici* protetti e delle corrispondenti *modalità di aggressione*. Orbene, si possono distinguere fondamentalmente tre gruppi di fattispecie incriminatrici: aggressioni a beni giuridici *tradizionali* attinti con nuove modalità o mezzi; aggressioni a beni giuridici senza dubbio *nuovi*[46]; una categoria intermedia che raggruppa aggressioni a beni giuridici *analoghi* a quelli tradizionali, ma che hanno una fisionomia dissimile per la diversità dei nuovi oggetti passivi o mezzi di esecuzione[47].

In realtà, ciò che va doverosamente evidenziato è che sono gli stessi interessi protetti ad essere modificati o condizionati dallo sviluppo e diffusione delle nuove tecnologie. Per tale ragione, è difficile parlare di beni realmente identici a quelli tradizionali, anche nel caso in cui non si tratti di beni radicalmente o totalmente nuovi.

La quotidiana circolazione, diffusione e utilizzazione dei dati, sistemi e prodotti elettronici hanno creato, si diceva, degli interessi totalmente nuovi ed articolati. L'importanza assegnata a tali *interessi* li ha resi anche degni di una protezione giuridica – specifica, autonoma ed anche penale - meritando una regolamentazione a livello tanto nazionale quanto sovrannazionale. Al riguardo, è corretto parlare di *beni* giuridici *nuovi,* perché essi non trovano una corrispondenza con quelli tradizionali.

Le categorie dei beni ai quali riallacciare questi nuovi interessi sono essenzialmente due: da un lato l'*integrità* e la *sicurezza* elettronica e, dall'altro, la *riservatezza* informatica intesa in senso stretto.

Il primo ordine d'interessi ha acquisito una notevole importanza pratica, e con essa una propria autonomia concettuale, per la crescente ampiezza dei

45 Paradigmatici: l'ingiuria, l'incitazione all'odio, alla violenza, la diffusione di materiale pornografico etc.

46 Ad esempio la sicurezza ed integrità dei *dati* e sistemi elettronici, la riservatezza informatica.

47 Ad esempio la fede pubblica nei documenti informatici falsi.

rapporti che si svolgono tramite le nuove tecnologie. Si tratta di preservare e garantire l'*utilizzabilità*, *fruibilità* o *disponibilità* dei dati, sistemi e prodotti elettronici dal pericolo di alterazione, distruzione, dispersione o impedimento, anche se temporanei. *Vulnera* questi, in grado di pregiudicare la *speditezza* e *correttezza* dei rapporti economici e sociali, indipendentemente dal fatto che si concreti, anche, la lesione di beni giuridici tradizionali che rimangono in secondo piano[48]. La *pronta* e *corretta* utilizzabilità dei nuovi mezzi informatici, dunque, diviene un valore da proteggere, anche penalmente, da condotte lesive che attentino i rapporti economici e sociali. L'esigenza di protezione si consacra nel nuovo paradigma della «*sicurezza informatica*», che, come specificazione del valore della *pronta e corretta utilizzabilità*, rimodella le peculiarità tecniche di incriminazione. Il menzionato paradigma individua un livello *anticipato e preventivo* di tutela rispetto all'effettiva lesione all'«*integrità*» ed «*utilizzabilità*» dei dati e sistemi elettronici ed abbraccia tutte le misure poste a sua difesa[49]. Il legislatore del 1993 configura in tal modo il delitto previsto dall'art. 615-*quinques* c.p.[50], strutturato come reato di pericolo che si consuma con la semplice *diffusione*, *comunicazione* o mera *consegna* di un programma *virus*, indipendentemente dalla verificazione del danneggiamento o dall'installazione o attivazione del *virus*. Ad integrare la fattispecie è sufficiente lo scopo o l'effetto di tale programma, non il dolo specifico ascritto all'agente[51].

Il nuovo bene della *riservatezza informatica* si fa largo nella maturata lettura dell'art. 615-*ter* c.p.[52] «*accesso non autorizzato a un sistema informatico e telematico*» la cui struttura viene modellata sulla falsariga dell'art. 614 c.p. «*violazione di domicilio*». La chiara lettera della Relazione ministeriale al disegno

48 Ad esempio il patrimonio, la fede pubblica, l'ordine pubblico, i diritti di esclusiva, la riservatezza domiciliare, personale o informatica etc.

49 Ad esempio i codici d'accesso, le *password*, gli *standard* di comportamento per gli operatori, utilizzatori e titolari o soggetti autorizzati a fruire di dati e sistemi.

50 Configurato nellla l. 547/93 come *delitto-ostacolo* a consumazione anticipata di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

51 L'articolo verrà modificato dalla l. 48/08 di ratifica ed esecuzione della Convenzione *Cybercrime* del 2001. Sulla formulazione dell'art. 615-quinquies c.p. ad opera della l. 547/93 si rinvia al Cap. III par. 4.1 e in particolare al caso Vierika § 5. L'articolo è stato riformulato dalla l. 48/08 che ha sostituito il requisito oggettivo della pericolosità dei programmi o dispositivi informatici con quello soggettivo del dolo specifico, si rinvia al Cap. IV § 5.

52 L'articolo, introdotto con la l. 547/93, non verrà modificato dalla l. 48/08.

di legge n. 2773 del 1993 esprimeva l'idea di tutelare i sistemi informatici e telematici in quanto «*espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 della Costituzione e penalmente tutelati nei suoi aspetti essenziali agli articoli 614 e 615 del codice penale*». La dichiarata analogia con il *domicilio*, bene eminentemente privato e personale, in realtà coglie solo parzialmente il contenuto dello *jus escludendi* dalle sfere di *disponibilità* e *rispetto nuove*, create o rese fruibili dall'innovazione tecnologica[53]. La tutela apprestata, in realtà, non riguarda né *privacy*, né dati personali, né il luogo, pur se virtuale. Il diritto di escludere altri, in effetti, si configura nel potere tutelato di gestire, autonomamente e in senso esclusivo, qualsiasi spazio che un soggetto abbia a disposizione, sia in sistemi informatici *stand alone* che connessi in *rete*[54]. Tale facoltà si specifica nella possibilità di elaborare, memorizzare, selezionare, trasmettere e trattare dati di qualsiasi contenuto, genere ed importanza e di metterli, o meno, a disposizione di altri. L'identità personale e l'autonomia delle scelte rimangono salvaguardate indirettamente, ma non rappresentano l'oggetto diretto della tutela. Orbene, l'estensione nell'utilizzo di *Internet* fa emergere la delimitazione ed il riconoscimento di confini per l'accessibilità ai *dati* e sistemi informatici "*altrui*". L'inosservanza di queste frontiere si ripercuote negativamente sulla *certezza dei rapporti* e sulla *sicurezza* delle relazioni che si svolgono per via informatica e telematica. La *riservatezza informatica* non è un interesse esclusivamente privato che dipende da una diligente difesa individuale, perché si proietta sul piano collettivo e crea uno stretto legame con un interesse sociale: la *sicurezza* e *certezza* delle relazioni giuridiche. L'importanza di questo *nuovo* interesse giuridico è positivamente dimostrata dalla fattispecie-ostacolo di cui all'art. 615-*quater* c.p., che punisce la mera detenzione e diffusione abusiva di codici d'accesso ai sistemi informatici o telematici o il fornire indicazioni o istruzioni al predetto scopo. Sono punite, dunque, condotte idonee a consentire l'accesso ai sistemi informatici e che sono solo meramente preparatorie o prodromiche alla lesione. L'oggettività giuridica non è esclusivamente correlata alla dimensione della *riservatezza informatica*, giacché abbraccia la tutela

53 Ovvero la sicurezza ed integrità dei dati e sistemi elettronici o la riservatezza informatica
54 Si rinvia al Cap. II, § 5.1, commento all'art. 2 CoC.

preventiva di altri beni, come il diritto di esclusiva su programmi per elaboratore, banche-dati, prodotti tutelati dal diritto d'autore. Il profilo della *sicurezza* (*incipit* dell'articolo in questione), grazie al suo carattere preventivo, emerge con un'intensità tale da farla apparire come bene giuridico assorbente. La funzione strumentale alla protezione di altri beni, in realtà, viene positivamente sanata dalla struttura a dolo specifico. La condotta, infatti, deve essere realizzata «*al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno*». Il requisito che il «*sistema informatico o telematico*» sia protetto da «*idonee misure di sicurezza*» diviene decisivo e riemerge la *riservatezza informatica* lesa dalle condotte di accesso *abusivo* o non autorizzato, indipendentemente dall'ulteriore fine che le ha determinate [55]. Orbene, l'oggetto principale della fattispecie di cui all'art. 615- *ter* c.p. «*accesso abusivo a un sistema informatico e telematico*» è l'interesse alla «*riservatezza*», ma, grazie al 2° comma n. 3, si viene a creare una stretta connessione tra diritto di escludere i terzi e i beni della «*sicurezza*» ed «*integrità*» informatiche[56]. L'articolo in questione, infatti, configura un'ipotesi di delitto aggravato nel caso in cui all'accesso abusivo consegua il danneggiamento dei *dati* o degli apparati elettronici ovvero l'interruzione, anche parziale, o la mera alterazione del funzionamento del sistema informatico o telematico. Il legislatore si preoccupa di precisare che tali eventi vanno di là del danneggiamento previsto nell'art. 635-*bis* c.p., includendovi i profili funzionali e propri della tutela dell'«*integrità*» e «*sicurezza*» informatiche. L'evento aggravatore: «*se dal fatto deriva la distruzione dei dati o del sistema o l'interruzione anche parziale del funzionamento*», in realtà integra la figura di un reato complesso, facendo presumere la possibilità d'imputazione anche a titolo di mera colpa, *ex* art. 59, 2° co., c.p., sempre che non si voglia, addirittura, ammettere una responsabilità a titolo oggettivo[57] con tutte le conseguenti implicazioni di natura costituzionale.[58]

E' doveroso ribadire che nel settore in argomento giocano un ruolo fondamentale le innovazioni tecniche e le ricadute nel mondo giuridico hanno un

55 Cfr. L. PICOTTI, *Sistematica*, cit., 70 ss.
56 Cfr. L. PICOTTI, ID, 75 -77
57 Cfr. MUCCIARELLI F., *Commento agli art. 1,2,4, e 10, L.23 dicembre 1993,* in *legisl.pen*, 1996, 57 ss.
58 V. PICOTTI L., *Reati informatici*, cit., 20.

impatto a volte devastante, giacché impongono ripensamenti di non facile percorso tanto in campo legislativo quanto giurisprudenziale e/o dottrinale[59].

Il quadro proposto dall'ordinamento italiano, in realtà non sempre facilmente decifrabile, si caratterizza per le previsioni frammentarie e settoriali. Le nuove incriminazioni e sanzioni penali, spesso, non sono concordate tra loro e/o con quelle preesistenti, quindi è difficile parlare di un sistema coerente[60].

L'iridescente ed incessante evoluzione nei modi di manifestazione delle svariate forme di criminalità informatica - dai classici *Computer crime* degli anni Ottanta - Novanta fino alle nuove e sofisticate forme di *Cybercrime* - altro non è che uno degli esiti più pericolosi della globalizzazione. Il menzionato fenomeno, indotto da *Internet* con le sue variegate forme di connettività e /o comunicazione, permette la circolazione capillare di *dati* di qualsiasi natura (suoni, immagini etc.) in quantità, qualità e rapidità poco tempo fa inimmaginabili. L'urgenza di garantire risposte rapide a fronte degli usi distorti delle nuove tecnologie, spesso, ha indotto soluzioni normative circoscritte a casi o settori specifici, anche quando l'intervento del legislatore fu reso necessario dall'esigenza di colmare vuoti legislativi o di dar seguito ad obblighi comunitari.

La congerie di norme, affastellatesi in materia, rappresenta il prezzo inevitabilmente pagato dal lungo processo di affermazione di quell'unità concettuale che giustifica, oggi, la denominazione autonoma di un *diritto penale dell'informatica*. Tale branca del diritto rappresenta un settore nuovo e con tratti specifici, frutto di una produzione legislativa e giurisprudenziale, come s'è visto, in espansione crescente[61]. D'altro canto, poi, sia la Raccomandazione R (89)9 del Consiglio d'Europa sia la Convenzione *Cybercrime* lasciavano ampi margini di discrezionalità nelle scelte di formulazione normativa delle fattispecie o del tipo ed estensione delle sanzioni. Ebbene, la tecnologia ha cambiato le modalità di commissione degli illeciti e di conseguenza l'impatto dei nuovi crimini sul tema del 'giuridicamente e penalmente tutelato'. Gli stessi crimini hanno subito un incremento, in misura più che proporzionale, dal momento in cui l'*automazione*

59 V. Caso Vierika, Cap. III, § 5.
60 Cfr. PICOTTI L., *Sistematica* , cit., 21 ss
61 Cfr. PICOTTI L., *Biens juridiques protegèe* , cit., 527.

degli attacchi è entrata a far parte dell'armamentario del criminale. I Paesi e le organizzazioni regionali ed internazionali hanno reagito alle crescenti difficoltà conferendo una priorità senza precedenti al fenomeno della *Cyber delinquenza*.[62] In estrema sintesi, l'epoca di *Internet* ha segnato il passaggio dalla categoria tradizionale del *Computer crime* a quella del *Cybercrime*. L'aggettivo *informatico* svela l'essenzialità del suo significato identificando le procedure di trattamento automatizzato di dati, comprese le comunicazioni a distanza in rete, ed attrae nell'alveo dei reati, ai quali l'aggettivo si accompagna, sia comportamenti diretti contro i prodotti e strumenti (*computer*, *smartphone*, *tablet* o tessere contenenti *microchips*) sia quelli che si realizzano nelle o tramite le reti (*web*, *cloud* ecc.). L'espressione *Computer crimes*, sebbene invalsa nel linguaggio giuridico, in realtà induce l'errata e riduttiva suggestione che la tutela penale abbia ad oggetto solo il *computer*; in senso opposto quella di *high-tech crime* – talora utilizzata dalla dottrina di *common law* – dà luogo ad un'eccessiva dilatazione dell'oggetto. Per tali motivi sarebbe più corretto usare l'espressione «*reato informatico*», capace di comprendere la molteplicità delle condotte illecite che via via mutano all'incedere del progresso tecnologico.

4. *Nuove problematiche dal Cyberspace: cenni alle questioni di giurisdizione correlate al Cloud computing.*

Dal punto di vista tecnologico fino agli Novanta tutti i *personal computer* vissero di " vita propria ", nel senso che non erano tra loro interconnessi. Dopo gli anni Novanta, l'avvento di *Internet* ha consentito di mettere in *rete* alcuni *personal computer* (ovviamente i più potenti: i *server*) col fine di velocizzarla, risultato che, di fatto, si ottenne. Orbene, in quegli anni comparve l'interfaccia grafica "*www*" e tale evento ha determinato, accanto all'incremento del numero degli internauti, dei nuovi problemi, tutt'oggi attuali. Le informazioni disponibili o trasmesse nella *rete*, legali o meno alla stregua della legislazione di un dato Paese, diventano fruibili, ma anche lesive, per ogni utente connesso da un qualsiasi luogo della Terra. In sostanza, *Internet* trasforma il delitto informatico, alla stregua della

62 Cfr. *Amplius*, GERCKE M., *Cyberdelito*, (contributo di) Fonte ITU settembre 2012.

legislazione di uno o molti Paesi, in un illecito a vocazione internazionale. Tal fatto ingenera problemi e difficoltà legate all'attività di investigazione ed accertamento da parte delle autorità di *law enforcement*, circostanza che da tempo aveva guadagnato l'interessamento sia degli organismi sovranzionali che della comunità scientifica. Paradigmatiche espressioni di siffatta preoccupazione furono: la Risoluzione 45/121, adottata dall'assemblea nazionale delle Nazioni Unite del 1990 ed il manuale per la prevenzione ed il controllo dei delitti informatici, pubblicato nel 1994[63]. Durante il XV Congresso *dell'Association International de droit pénal* (A.I.D.P.) del 1994[64], poi, gli studiosi espressero l'idea di considerare unitaria la lista delle condotte di abuso informatico previste dalla Raccomandazione del Consiglio d'Europa, ne aggiornarono le indicazioni. Il Congresso rappresentò, dunque, l'occasione per sollecitare l'ampliamento delle fattispecie di illecito informativo con particolare riferimento ai danneggiamenti derivanti dall'utilizzo di programmi *virus*, non considerati dal Consiglio d'Europa. Giunti alla prima decade del nuovo millennio, infatti, s'impongono all'attenzione di tutta la comunità scientifica e politica nuovi e sofisticati metodi per la commissione di illeciti elettonici, tra essi il *Phising* e le cd. *reti zombi* (o *Botnet*).

Da altro punto di vista, la comunicazione *VOIP* e la memorizzazione dei *dati* elettronici nella cd. "*Nube*" (o *Cloud*) lanciano nuove sfide all'investigazione e, di conseguenza, alla possibilità di accertare gli illeciti in quell'ambito.

Il *Cybercrime*, ormai uscito dalla fase embrionale, si propone, oggi, come paradigma del modo col quale viene utilizzata la tecnologia dell'informazione. Se è vero che l'uso lecito dei nuovi strumenti potenzia la comunicazione e la gestione dei rapporti privati, economici ed istituzionali, quello illecito lucra o sfrutta, in modo distorto, i predetti benefici. I criminali, poi, spesso sono i primi ad individuare e sfruttare le scappatoie e gli effetti delle nuove tecnologie. Uno degli usi più interessanti e al contempo problematici della nuova forme di comunicazione e memorizzazione è *Cloud accounting system*[65]. I *Cloud*, *server*

63 Attualmente consultabile all'indirizzo: http://www.uncjin.org/Documents/irpc4344.pdf.

64 Per un approfondito commento critico della risoluzione dell'A.I.D.P. vedasi: PICOTTI L., *Le «Raccomandazioni» del XV Congresso Internazionale di diritto penale in tema di criminalità informatica,* in *Riv. trim. dir. pen. econ.*, n. 4, 1995, 1279.

65 Fonte, *http://it.wikipedia.org/wiki/Cloud_computing*: «In informatica con il termine inglese

collegati tra loro fino a formare una *nube* di *computer*, consentono infatti agli utenti il collegamento ai *dati*, contenuti in quest'ultima, da un qualsiasi luogo, territorialmente inteso. Tramite la menzionata innovazione è possibile fruire di un'innumerevole quantità di servizi[66] oppure della semplice memorizzazione dei *dati* in un luogo esterno alla macchina, sia essa un *personal computer*, un *tablet* o uno *smartphone*. Grazie al modello tecnologico-informatico del *client/server,* le operazioni di calcolo, memorizzazione dati, distribuzione di *software* etc. avvengono all'interno della *Nube*. La novità, sebbene consenta di minimizzare i costi di gestione dei dati ed incrementare il livello della prestazione e/o godimento dei servizi, aumentando anche il livello di affidabilità, determina un'innumerevole quantità di problemi dal punto di vista giuridico, soprattutto in ambito procedurale.

Un primo problema pratico: il servizio *Cloud* sfrutta la potenzialità di *servers* che si trovano, sì, nella *Nube*, ma dislocati fisicamente nel territorio sovrano di pressoché tutti i Paesi della Terra. In fase di *trattamento,* il flusso dei *dati* si sposta in continuazione all'interno della *Nube*, migrando da un *server* all'altro. Il *file,* memorizzato nella cartella del *Cloud*, sempre ed in ogni momento accessibile dall'utente, in realtà non può mai essere localizzato con assoluta certezza su un determinato *server* fisicamente collocato sul territorio sovrano di un preciso Stato. Questa implicazione determina, in prima battuta, un problema di competenza giurisdizionale e di legge applicabile.

In senso pragmatico, ipotizziamo che un'immagine pedopornografica venga 'postata' sul *Cloud*, poi modificata ed infine cancellata dall'autore. Di là della questione se il fatto sia lecito o meno, alla stregua dell'ordinamento dello Stato al quale appartiene il responsabile, quella stessa fotografia viene immediatamente "*trattata*" da *server* che fanno parte della *rete*, ossia collocata nello spazio indefinito denominato *Nube* o *Nuvola*. L'effige quindi, pur se modificata e poi definitivamente cancellata dall'autore, potrebbe essere presente, magari in

---

Cloud Computing (in italiano nuvola informatica) s'intende un insieme di tecnologie che permettono, tipicamente sotto forma di un servizio offerto da un *Provider* al cliente, di memorizzare/archiviare e/o elaborare dati (tramite *CPU* o *software*) grazie all'utilizzo di risorse *hardware*/*software* distribuite e virtualizzate in *rete* in un'architettura tipica *client-server*».

66 Ad esempio il collegamento alle banche-dati, le operazioni bancarie, il *download* di materiale audio/visivo, *software*, gestione di tale materiale etc.

versioni diverse, all'interno dei vari *server* che compongono la *Nuvola*. Il fenomeno che si verifica può essere efficacemente descritto con l'espressione linguistica: '*perdita di localizzazione univoca del file*', fatto che deriva, appunto, dal costante spostamento del flusso di informazioni/dati all'interno del *Cloud*. Il *provider Cloud computing* (ad esempio *Google*) potrebbe, sì, fornire l'ultima versione dell'immagine pedopornografica passata tramite il suo *server*, ma non è detto che quella sia la versione voluta *attualmente* dall'autore. Paradossalmente, nemmeno quest'ultimo è in grado di sapere, dove sia esattamente il *file* che l'utente vede sul *desktop* del *personal computer* e, poiché la *Nube* nega il concetto tradizionale di spazio fisico, quest'ultimo può solo avere la certezza che l'immagine sia nel *Cyberspace*. I *files*, costantemente spostati nel *Cloud* da un *server* all'altro, invero potrebbero essere duplicati da un determinato *server* per ragioni di sicurezza: dunque, copie diverse potrebbero essere contestualmente presenti in più *server* all'interno di uno stesso Stato o di Stati diversi. Per queste ragioni, nemmeno il *provider* del *Cloud computing* sa esattamente dove ricercare i *files* e, soprattutto, dove si trovino in un preciso momento.

L'indeterminatezza che affligge la competenza giurisdizionale si ripercuote inevitabilmente sulla legittimazione dell'autorità inquirente in ordine alla possibilità di ottenere l'accesso ai *dati* presenti nella *Nube*.

La collocazione territoriale, elemento applicabile, in realtà, a tutte le cose tangibili ed anche agli oggetti immateriali al momento dell'implementazione dell'*Internet*, diventa una nozione inutile se rapportata al *Cloud computing*.

Il criterio di territorialità, però, è di primaria importanza, poiché consente di determinare la competenza giurisdizionale, la legge applicabile, e, in particolare, l'esercizio dei poteri coercitivi necessari per recuperare l'eventuale oggetto del reato, quindi ai fini della ricerca e raccolta delle prove.

Sul piano internazionale la sovranità territoriale è espressa nel principio secondo il quale nessuno Stato può imporre la propria giurisdizione sul territorio di un altro Stato sovrano. E' altrettanto vero che, nel campo delle indagini, questo postulato potrebbe essere salvaguardato, giacché esistono gli strumenti di mutua assistenza e di cooperazione. Tuttavia, poiché la localizzazione spaziale dei *dati* spesso non può essere determinata, né attualmente né nel futuro, la

determinazione della competenza giurisdizionale sarebbe consacrata solo se vi fosse una sicura corrispondenza tra *data* e il *client-cloud* (meglio la persona fisica). La sicura localizzazione spaziale, in realtà, non fa venir meno il rischio di *forum shopping*. Quest'esito incerto mal si adatta alle esigenze di uno Stato di diritto che vanno salvaguardate soprattutto in ambito penale. La difficoltà nel delineare una sicura competenza territoriale, tuttavia, non può sminuire l'importanza di perseguire i *Cybercrimes*, date la loro dimensione, potenzialmente globale, e l'ampiezza degli interessi lesi (privati, istituzionali).

Il diritto penale internazionale, invero, conosce il principio non solo di territorialità, che è il fondamentale elemento di collegamento per l'esercizio legittimo del potere sovrano, ma anche delle deroghe: il principio degli *effetti*, quello di *bandiera* e quello di *nazionalità*. Ora, se il principio di territorialità è l'ostacolo primario per indagare su ciò che d'illecito si compie nelle *Nubi*, forse le deroghe potrebbero rivelarsi strumenti utili per un diverso approccio, così da consentire alle autorità investigative di ottenere, in modo legale, quei dati critici (identificazione univoca dato/file/informazione e persona fisica) dai fornitori di *Cloud computing*.

Se è vero che le autorità di uno Stato perseguono il crimine informatico solo quando abbiano già assunta la giurisdizione, è anche vero che il criterio degli *effetti* non può fungere da modello ispiratore per determinare la competenza giurisdizionale.

In realtà, nella Convenzione di Budapest[67] sulla criminalità informatica si trovano riflessi due princìpi di diritto internazionale: quello della *bandiera* (art. 22 lett. b e c) e quello della *nazionalità* (art. 22 lett.d).

Il primo di questi principi afferma che i crimini commessi a bordo di navi, aeromobili e veicoli spaziali sono soggetti alla giurisdizione dello Stato di bandiera; la competenza viene legata ad un oggetto fisico (la nave o l'aereo). Il principio di *bandiera*, in sostanza, crea un'estensione fittizia del territorio sovrano e permette di perseguire l'illecito penale secondo la legge dello Stato che marca con la propria insegna l'oggetto, indipendentemente dal luogo in cui è stato

[67] Sia gli articoli che la stessa Convenzione *Cybercrime* saranno di seguito indicati anche con l'acronimo CoC.

fisicamente commesso il fatto. Quest'idea potrebbe essere feconda se applicata allo scenario del *Cloud computing*, salvo aver chiaro in mente che la *Nube* potrebbe non essere il luogo di effettiva commissione dell'illecito. A quest'ultima differenza concettuale se ne aggiunge un'altra, ossia l'assenza di un elemento o supporto fisico da ricercare. Tra l'aeromobile in volo, una nave in alto mare e i *dati* nella *Nube,* tuttavia, c'è una certa vicinanza: tutti sono in costante movimento. Tramite l'uso di *metadati*[68], in alcuni casi è possibile determinare lo 'Stato di bandiera'[69]. Tale approccio, in realtà, non è di sicuro successo, poiché si tratta di *dati* facilmente modificabili; ne consegue che l'applicazione del criterio della bandiera non fornisce una valida soluzione per aggirare le questioni di territorialità sollecitate dall'ipotesi in argomento.

Il secondo principio, ossia quello di *nazionalità,* stabilisce che la cittadinanza del colpevole è criterio di collegamento legale per determinare la giurisdizione penale, secondo il brocardo *aut dedere, aut iudicare*. Tale assioma pone altri gravi e preoccupanti problemi: gli autori di un *Cybercrime* potrebbero essere dei cittadini stranieri, ma la criminalità informatica non richiede una vicinanza fisica, inoltre la nazionalità non è qualità attribuibile ai *dati*. In altre parole, la *nazionalità* è un attributo della persona che, se autore di un reato, deve poter essere ricollegata ai *dati*, ma a questi ultimi non si attaglia quel carattere. Il solo criterio della *nazionalità*, dunque, non è in grado di realizzare il requisito di collegamento persona/dato. In sostanza si verifica un fenomeno che potremmo descrivere con l'espressione '*perdita d'identificazione univoca del file*'.

Il *Cyberspace*, invero, annulla e nega la fisicità ed i confini, anche se la sua esistenza deriva da elementi fisici: macchine, infrastrutture, cavi collegati fisicamente e collocati sul territorio di una gran quantità di Stati. L'*Internet*, mezzo veramente transnazionale, nega l'esistenza di limiti e confini, crea una dimensione distinta dal territorio fisico con i propri confini sovrani. Il *Cyberspace* e/o la *Nube* evocano sia una dimensione marittima (navigare in *Internet*) sia spaziale (web space -*Nube*) tanto da indurre la suggestione di estendere la ricerca di modelli in tali campi. Entrambi questi «*luoghi*» – l'alto mare e lo spazio – sono presi in

68 Trattasi delle cosiddette *informazioni aggiuntive di catalogo*.
69 Ad esempio tramite le immagini geo-referenziate, i documenti assegnati geograficamente etc.

considerazione dal diritto internazionale, dai trattati e dal principio di territorialità ai fini della determinazione della giurisdizione.

Nel *Cloud computing*, dove i *dati* si trovano localizzati in *Nubi*, si presentano le stesse condizioni delle navi in alto mare o delle astronavi nello spazio. I trattati internazionali prevedono che la responsabilità penale per i danni derivanti da veicoli spaziali (satelliti – navicelle) faccia capo allo Stato in cui il veicolo è stato registrato. Un siffatto ragionamento potrebbe attagliarsi al sistema d'identificazione tramite I.P. (*Internet Protocol Address*), che identifica l'indirizzo posseduto da un dato dispositivo (*router, modem*) al momento del collegamento ad *Internet*, con l'avvertenza che esso non è in grado di creare una sicura connessione tra il dato e la persona. Non va, infatti, tralasciato il problema degli attacchi *Sproofing*[70] o *Network sniffing*[71]. L'accordo sulla Stazione Spaziale Internazionale specifica che la giurisdizione penale all'interno della S.S.I.[72] è determinata, in parte, dal principio di *bandiera*[73] e, in parte, dal principio di *nazionalità*. Si prevede che, qualora il cittadino di un Paese *partner* infligga danni al cittadino di un'altra Nazione *partner*, gli Stati siano tenuti a una reciproca consultazione per giungere ad un accordo sulla giurisdizione penale. Consta però che non è dato trovare delle regole procedurali che stabiliscano la competenza per i reati commessi fuori dalle navi, stazioni o veicoli spaziali e che, quindi, possano fungere da paradigma per descrivere il fenomeno di delocalizzazione spazio-temporale che si verifica nel *Cloud computing*.

Allo stato attuale, la possibilità di accedere ai dati personali collocati nel *Cloud* ai fini investigativi necessita del consenso dell'interessato. Risolvere il problema in questione, esclusa l'ipotesi di potervi adattare modelli presenti nel diritto internazionale, impone di ricercare altrove il criterio legale di collegamento *dato/persona* che giustifichi e legittimi l'accesso al *Cloud-account* qualora sorga il

70 Lo *Spoofing* è l'usurpazione dell'identità di un soggetto o di una macchina. Tecnicamente si realizza con la falsificazione l'*IP address* di una macchina (X) in modo da farla apparire un'altra (Y) e superare, in questo modo, la difesa basata su tale controllo (ad esempio, la regola di un *firewall*)

71 Lo *Sniffing* è l'ascolto in *rete* e la cattura dei *dati* che vengono trasmessi tramite quest'ultima. Per l'attuazione tecnica è previamente necessario l'aver preso il controllo di una macchina che fa parte della *rete* alla quale appartiene quella bersaglio.

72 La S.S.I. è presa ad esempio in quanto è attualmente l'unico oggetto presidiato nello spazio esterno che non è considerato veicolo spaziale.

73 In riferimento allo Stato di registrazione di ciascun componente.

fondato sospetto che si stia per commettere, o sia stato consumato, un illecito di rilevanza penale. L'unico approccio percorribile è, dunque, di ordine procedurale, salve le garanzie dei diritti fondamentali dell'indagato, con 'accessi' consentiti limitatamente ai casi urgenti, giacché è notoria la riluttanza degli Stati ad accettare l'esercizio di misure coercitive da parte di altri Stati sul proprio territorio sovrano.

A ben vedere, un tal elemento esiste ed ha i connotati del potere dispositivo che fa capo ai fruitori dei servizi *Cloud*. Tali soggetti ottengono, tramite le credenziali fornite dal *provider*, l'accesso al *Cloud* e detengono il diritto di modificare, cancellare, sopprimere o rendere inutilizzabili i *dati* contenuti nel proprio *account,* così come il diritto di escludere altri da accessi od utilizzi non autorizzati. Tale potere di disposizione, previsto e tutelato dall'art. 2 CoC[74] e dall'art. 4 CoC[75], rappresenta un parametro proprio dell'informatica. Esso consente di compiere legittimamente le suddette operazioni di accesso/gestione dei *dati*; per queste ragioni esso rappresenta un mezzo utilizzabile anche ai fini delle indagini onde stabilire il collegamento tra le procedure d'identificazione (dati personali) e i *dati* elettronici. Si tratta di un principio di collegamento, indipendente dalla dimensione spazio-temporale, indispensabile per fruire dei servizi di *Cloud computing,* poiché i fornitori sono tenuti a memorizzare i dati di milioni di utenti separatamente e a mantenere l'allocazione/identificazione del *client*. Questa procedura, fondata sulla creazione del collegamento dato-persona, è implementata dalla possibilità di accedere ai dati elettronici immagazzinati, indipendentemente dal luogo in cui si trovano. E' doveroso ribadire che l'esatta posizione di questi ultimi potrebbe essere sconosciuta od incerta a causa dell'utilizzo della tecnologia *Cloud computing*.

Ai fini delle indagini, quest'aspetto potrebbe non essere significativo, nel caso in cui siano soddisfatti alcuni requisiti supplementari e cumulativi: a) l'accesso deve essere avvenuto con credenziali che eseguano un'appropriata identificazione; b) le credenziali devono appartenere o essere utilizzate dal sospetto criminale ed essere ottenute in modo lecito; c) non ci deve essere stato

74 L'art. 2 CoC disciplina l'accesso illegale ad un sistema informatico/*system interference*.
75 L'art. 4 CoC disciplina l'attentato all'integrità dei dati/*data interference*.

alcun aiuto da parte del fornitore di *Cloud computing*; d) il sospetto deve essere fisicamente sul territorio dell'autorità inquirente o avere la sua stessa nazionalità. Qualora concorrano tutte le predette condizioni, si potrà dire che sia teoricamente soddisfatto il requisito d'identificazione univoca dato/persona fisica. Alle autorità residuerebbe solo l'onere di ottenere, in modo legale, *userid* e *password* e di dimostrare che i requisiti supplementari siano soddisfatti.

Una tal procedura, invero, è passibile di violare i diritti degli indagati e/o dei terzi; non sarebbe lecito, d'altro canto, leggere i pensieri intimi, postati su un *account* come *Evernote* o *Dropbox*, da chi sia indagato per una presunta diffamazione. Nella *Nube*, solitamente, vengono memorizzati dati dai contenuti più svariati (*files*, *mail*, video etc.) che sono oggetto di una speciale protezione in numerosi Paesi. L'accesso abusivo ad un *account* di posta elettronica è violazione del diritto alla segretezza delle *comunicazioni*, salvo che intervenga la previa autorizzazione del giudice competente. D'altro canto, l'art. 15 CoC – nell'ambito delle procedure penali – prevede che «*Ogni Parte che provvede deve assicurarsi che l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste in questa sezione siano soggette alle condizioni e alle tutele previste dal proprio diritto interno, che deve assicurare un'adeguata tutela dei diritti umani e delle libertà, in particolare dei diritti derivanti da obblighi assunti in base alla Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e delle libertà fondamentali, alla Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici, e agli altri strumenti internazionali applicabili in materia di diritti umani, e che deve considerare il principio di proporzionalità*».

La nascita e lo sviluppo del *Cloud computing*, se da un lato hanno favorito il nascere di nuove opportunità criminogene, dall'altro hanno avuto la capacità di spiazzare gli organi investigativi a causa del fenomeno della diversa dislocazione spazio-temporale derivante da detta tecnologia. I concetti di territorialità e competenza, criteri di collegamento legale privilegiati per le attività investigative, rimangono svuotati di senso in rapporto alla nuova entità – *la Nube/Cloud* - mentre si fa largo la necessità di affinare gli strumenti d'indagine per assicurare alla giustizia chi commetta un delitto in quel contesto. La questione è ancora fortemente dibattuta e non si è giunti ad approdi sicuri proprio per l'incessante

evolversi delle forme di criminalità che si compiono in tale scenario.[76]

76 V. *Amplius*, rapporto SPOENLE, *Discussion paper, Project on Cybercrime - Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?, www.coe.int/cybercrime Economic Crime Division Directorate General of Human Rights and Legal Affairs Strasbourg*, France, Version 31 August 2010.