Lorenzo Picotti (*)

Reati informatici, riservatezza, identità digitale

SOMMARIO: 1. *Premessa generale sulla "rivoluzione cibernetica"* – 2. *Lo specifico impatto delle TIC sul diritto penale* – 3. *Sui nuovi beni giuridici in specie della riservatezza informatica e della sicurezza informatica:* 3.1. *Varietà di beni giuridici offendibili nel* Cyberspace *ed esigenze di tutela delle vittime* - 3.2. *La riservatezza informatica* - 3.3. *La sicurezza informatica* – 4. *I singoli reati:* 4.1. *Accesso abusivo (art. 615-*ter *c.p.)* – 4.2. *Reati c.d. prodromici o preparatori:* 4.2.1. *La diffusione e detenzione abusive di dispositivi d'accesso (art. 615-*quater *c.p.)* – 4.2.2. *La diffusione e detenzione abusive di* malware *(art. 615-*quinquies *c.p.)* - 4.3. *La corrispondenza informatica* – 4.4. *Le "altre comunicazioni" a distanza* – 4.5. *Il "furto d'identità digitale" fra tutela del patrimonio e tutela della persona:* 4.5.1. *Formulazione tecnica delle "modalità di realizzazione" delle condotte tipiche* – 4.5.2. *L'assenza di una definizione di "identità digitale"* - 4.5.3. *Il bene giuridico protetto* - 5. *Osservazioni conclusive: verso un mutamento di nozioni basilari quale quella di consumazione del reato nel* Cyberspace*?*

(*) con il contributo di Ivan Salvadori (par. 4.2) e Roberto Flor (par. 4.5)

1. Premessa generale sulla "rivoluzione cibernetica"

La rivoluzione tecnologica, o meglio "cibernetica", ha avuto un forte impatto sui rapporti sociali e giuridici, determinando in circa mezzo secolo profondi cambiamenti anche per il diritto penale. Il primo elemento di novità, avente forti ricadute sull'ordinamento giuridico, è costituito dall'automazione, che ha via via sostituito porzioni progressivamente più estese ed importanti delle attività dell'uomo, come è riconosciuto anche nelle definizioni giuridiche di "dati" e "sistemi informatici" contenute nelle fonti sovranazionali (Convenzione Cybercrime del 2001; Direttìva UE del 2013).

L'apertura di Internet al pubblico a metà degli anni '90 dello scorso secolo ha poi trasformato le reti di comunicazione in una dimensione globale, che grazie anche ai dispositivi mobili ed all'estensione delle coperture di connessione, rappresenta oggi uno "spazio" di costante comunicazione e scambio, il c.d. *Cyberspace*, nel quale si dislocano sempre più attività individuali e collettive di ogni tipo, dal tempo libero, al commercio, dall'economia, alla cultura, fino alla politica. In tale spazio cibernetico gli utenti possono essere al contempo autori e vittime di reati e di comportamenti illeciti, per la struttura interattiva che la Rete ha via via assunto e la crescente estensione ed importanza dei contenuti e dei dati da essi stessi caricati, diffusi e scambiati, che vengono memorizzati, elaborati e gestiti su piattaforme informatiche e reti sociali da sistemi esperti e motori di ricerca sempre più potenti, determinando una progressiva concentrazione di poteri in capo agli *Internet Service Provider* (ISP) che ne siano titolari e li controllino.

Il riflesso immediato di questa "rivoluzione cibernetica" sul diritto penale è rappresentato dal passaggio dal concetto di *Computer crime* (reato informatico) a quello di *Cyebrcrime* (reato cibernetico), di cui va sottolineata l'espansione crescente. Accanto ai "reati informatici in senso stretto" – che sono connotati dalla previsione, nella fattispecie legale, di specifici elementi di tipizzazione, contenenti un esplicito riferimento alle nuove tecnologie dell'informazione o della comunicazione (c.d. TIC), siano essi relativi alla condotta od ai mezzi, alle modalità, agli effetti o ad ogni altro elemento essenziale o circostanziale: esempi classici sono l'accesso abusivo ad un sistema

informatico, la frode informatica, il falso in documenti informatici - sono oggi commissibili tramite oppure a danno di sistemi e strumenti informatici o, comunque, "nel" *Cyberspace*, reati di ogni altro tipo, i cui elementi costitutivi o circostanziali, in via alternativa od interpretativa, consentono in ogni caso di sussumerli nelle pertinenti fattispecie legali. Può quindi parlarsi di "reati informatici in senso ampio", o meglio di "reati cibernetici", che ricomprendono tutti quelli la cui commissione si realizzi o possa realizzarsi in Rete, potendo la stessa essere sia un elemento espresso che un elemento solo interpretativamente compatibile con la fattispecie legale (si pensi alla diffamazione *on-line*, alla diffusione di materiale pedopornografico, all'istigazione alla discriminazione ed all'odio razziale, ma anche ad estorsioni, riciclaggio, reati di violazione della *privacy* e dei diritti d'autore, ecc.).
Anche la collocazione sistematica di queste diverse categorie di reati informatici e cibernetici, ormai ampiamente presenti nel codice penale e nella legislazione speciale (in specie in materia di protezione dei dati personali e di diritti d'autore), evidenzia la grande varietà ed importanza dei beni giuridici protetti, che peraltro possono presentare, nella nuova dimensione cibernetica, specifici profili di novità, come emerge in termini chiari nel caso dei reati contro la riservatezza informatica e la sicurezza informatica.

2. Lo specifico impatto delle TIC sul diritto penale

Il *novum* che più investe sotto il profilo dogmatico la configurazione dei reati informatici e cibernetici, e dunque molte categorie penalistiche, è che l'informatica, ed ancor più quindi il suo sviluppo nella cibernetica, penetrano fino alla radice dell'agire dell'uomo, andando ben oltre lo svolgimento "meccanizzato" di operazioni matematiche (come era nell'originario approccio in cui si parlava di semplici "*calcolatori* elettronici", sviluppati a partire dalla c.d. macchina di Turing), per toccarne tratti ben più caratterizzanti, quali in specie:

1) le capacità *cognitive*, vale a dire di conoscere ed apprendere dall'esperienza del mondo "esterno", ricercando ed acquisendo direttamente informazioni e dati, come si verifica nei c.d. sistemi esperti, che individuano, riconoscono e memorizzano ogni sorta d'informazioni, immagini, suoni, utili ai fini della successiva *elaborazione automatizzata* (paradigmatici sono i sistemi di riconoscimento non solo di impronte, di visi e di voci, ma anche di comportamenti anomali o situazioni di pericolo, ad es. nel percorso di aeromobili e di veicoli, ovvero in luoghi pubblici quali aeroporti, stazioni ferroviarie, ecc.);

2) la capacità, ancor più rilevante, strettamente connessa con le predette, di *auto-determinarsi* di conseguenza, sulla base dell'elaborazione o, se si vuole, "conoscenza" e selezione (a sua volta *automatizzate*) dei dati e delle informazioni utili da considerare, esprimendo ed attuando immediatamente "decisioni" e *scelte operative*, fra possibili opzioni alternative. Per cui si parla a buon diritto di "intelligenza artificiale", che a partire dalle applicazioni più note dei motori di ricerca – capaci di indicizzare e personalizzare, sulla base di frequenze, preferenze e correlazioni acquisite dalle ricerche e dai dati lasciati dagli utenti stessi (compresi *cookies* di vario genere) od anche ormai dagli oggetti (il c.d. *IoT*: *Inernet of Things*, letteralmente: Internet delle cose) le informazioni più utili per offrire, ad es., le pubblicità più incisive in termini individualizzati, individuare o correggere errori o malfunzionamenti o necessità di aggiornamento, indicare i gruppi sociali di "amici" aventi interessi simili cui aderire, ecc. – vanno fino a quelle più sofisticate applicate alla robotica, alla domotica, alla guida di veicoli (compresi aerei, droni, missili, ecc.), ovvero al campo medico (in specie grazie alla c.d. telemedicina), bellico, ecc.

Oggi può parlarsi di un *equivalente* della "volontà" umana, espressa dai computer o, meglio, dai "sistemi" informatici (cibernetici), che trova già paradigmatici ed espressi riconoscimenti giuridici, di rilievo anche penale, concernenti ad es. la validità di atti, negozi, documenti, compresi i contratti, posti in essere e conclusi automaticamente da detti sistemi (come avviene quotidianamente nelle negoziazioni di borsa), che le persone (fisiche o giuridiche), cui si imputano quali "titolari", non avrebbero però potuto porre in essere negli stessi tempi, modi e contenuti[1].

[1] È sintomatica di questa inevitabile tendenza la cautela con cui l'ordinamento giuridico limita, ma nel contempo riconosce in ipotesi

Le nuove esigenze di specifica regolazione e tutela giuridica, di fronte a queste nuove realtà, per quanto riguarda gli aspetti penali, sono bene rappresentate dalla paradigmatica previsione del delitto di "frode informatica" (art. 640-*ter* c.p.), introdotto fin dal 1993 sulla base delle fonti e dell'esperienza internazionali, in cui l'attività "manipolatrice" dell'autore, latamente intesa, s'indirizza *direttamente* al sistema informatico e determina l'esecuzione di "atti dispositivi" di contenuto patrimoniale, che non transitano perciò da una previa o contestuale decisione di una vittima in carne ed ossa, la quale - pur restando titolare del bene giuridico offeso - non coopera personalmente al proprio danno, come prevede invece la fattispecie comune della truffa (art. 640 c.p.). Ma altrettanto significativi sono i delitti di falsità in "documenti informatici", che concernono "documenti" *prodotti* – in tutto o in parte – e comunque trattati dai sistemi informatici, anziché redatti da un uomo, cui va riconosciuto equivalente valore probatorio nel traffico giuridico e, quindi, corrispondente tutela penale (art. 491-*bis* c.p.). Per non parlare dell'emblematica incriminazione del delitto di "accesso abusivo" ad un sistema informatico (art. 615-*ter* c.p., su cui *infra* § 4.1.), che colpisce "azioni" irriducibili al paradigma fisico-corporale di un movimento muscolare dell'uomo, perché *immediatamente* dirette ai sistemi informatici con comandi veicolati e spesso programmati anche su larga scala dal *software*, capaci di eluderne le misure di protezione e di "penetrarvi", per compiervi ulteriori "azioni" di analoga natura, non concepibili né realizzabili se non tramite la tecnologia informatica. Altrettanto dicasi delle intercettazioni di comunicazioni informatiche (artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p.), che – a differenza di quelle telefoniche e telegrafiche - prescindono dal coinvolgimento di persone fisiche, che ne siano parte; e così via per ogni altro "reato informatico" (e cibernetico) di cui meglio si dirà (cfr. *infra* § 4).

3. Sui nuovi beni giuridici in specie della riservatezza informatica e della sicurezza informatica

3.1. *Varietà di beni giuridici offendibili nel* Cyberspace *ed esigenze di tutela delle vittime.*

Di fronte alla nuova realtà è cambiato di passo l'approccio alla criminalità informatica, a sua volta divenuta "criminalità cibernetica" o, meglio, criminalità "nel" *Cyberspace*.

Tale categoria non può essere più circoscritta ad un numero chiuso o limitato di reati e, quindi, di vittime potenziali, che suscitava l'interesse soltanto degli specialisti dei delitti ad alta tecnologia (TIC), ma include oggi una crescente e potenzialmente indefinita molteplicità di illeciti e di modalità di offesa di diritti ed interessi altrui, taluni anche di nuova creazione, in quanto frutto dello stesso sviluppo tecnologico. Esemplificando: è un "nuovo" crimine cibernetico (in senso ampio), se ed in quanto realizzato nel *Cyberspace*, l'estorsione commessa con la criptazione illecita dei dati di un sistema informatico altrui, tramite un *malware* abusivamente installatovi da remoto, che realizzi così una forma di *violenza* c.d. informatica – quale definita dall'art. 392, comma 3 c.p., aggiunto dalla L. 547/1993 – per mezzo della quale la vittima è "*costretta*", per riacquistare la libera disponibilità dei propri dati, a corrispondere un prezzo ingiusto di riscatto (spesso esigito in *bitcoin* od altra valuta virtuale da corrispondere o trasferire nel c.d. *dark web*), per ottenere l'indispensabile chiave di decriptazione, consumandosi in tal modo, con il duplice evento di profitto ingiusto e di danno altrui, consapevolmente voluti dall'agente, il delitto di cui all'art. 629 c.p.

Emerge, dunque, la grande novità, estensione e varietà delle modalità di condotta e delle tecniche di commissione dei reati cibernetici, la cui rapida evoluzione segue quella del *Cyberspace*, andando ben oltre l'ambito di quelli consistenti nella "comunicazione" o "diffusione" di un pensiero o di contenuti illeciti in rete, che pur vi mantengono un ruolo di grande rilievo.

---

sempre più estese, l'efficacia giuridica di decisioni "interamente" automatizzate che coinvolgano diritti ed interessi delle persone: si veda già l'art. 15 Direttiva europea 95/46 ed ora l'art. 22 GDPR secondo il cui par. 1. "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona", mentre nel par. 2 è elencata una serie assai ampia di eccezioni e condizioni, che sono molto meno stringenti nella corrispondente previsione dell'art. 11 Direttiva UE 680/2016 del 27.04.2016 sul trattamento di dati per fini di indagini e accertamento di reati.

E si ha una corrispondente espansione e diversificazione dei *beni giuridici* meritevoli di tutela penale e, parallelamente, delle vittime da proteggere, che ne sono titolari, spesso ignare o "vulnerabili", siano esse individui ovvero entità o categorie collettive, a partire dai minori fino a quelle esposte a discriminazioni, nonché più in generale – applicando la definizione della Direttiva europea in materia – "*non aventi cittadinanza*" negli Stati membri in cui il reato cibernetico, che è strutturalmente transnazionale, è commesso[2].

3.2. *La riservatezza informatica.*

Emblematica è proprio l'esigenza di specifica tutela penale della riservatezza nel *Cyberspace*.

Da un lato essa assurge alla nuova dimensione della "riservatezza informatica", quale autonomo bene giuridico ed, anzi, diritto fondamentale della persona, da intendere come diritto ad uno *spazio* informatico *esclusivo*, che a prescindere dai contenuti che vi siano presenti, trattati o comunicati, deve essere lasciato *libero da intrusioni* e manomissioni di terzi, in quanto strumento essenziale per la piena realizzazione della persona nell'odierna vita individuale e sociale, che neppure l'Autorità pubblica può violare o comprimere, se non nei casi e modi previsti tassativamente dalla legge e con le garanzie del controllo giudiziario[3].

Dall'altro, si distingue dalla *privacy* in senso stretto, che indica il più specifico diritto alla tutela dei *propri* "dati personali", ovunque e da chiunque siano rispettivamente localizzati o trattati, che ha assunto caratteristiche e dimensioni peculiari - rispetto all'originaria categoria di derivazione anglosassone, concepita quale difesa della vita privata (diritto ad essere "lasciati soli") dalle intrusioni ingiustificate dei nuovi *mass media*, all'epoca rappresentati dalla stampa[4] – richiedendo oggi nuove e complesse discipline di tutela, finalizzate a garantire la possibilità di "controllo" da parte della persona cui si riferiscono le informazioni ed il bilanciamento con la contrapposta esigenza di circolazione e di accessibilità anche da parte di terzi, in quanto elementi spesso essenziali per infinite attività e servizi in ogni settore della società contemporanea[5]. Le TIC ne hanno infatti determinato, per un verso, la grande estensione e facilità di raccolta e trattamento, per l'altro, l'importanza fondamentale per lo svolgersi di molteplici attività e rapporti – non solo nel *Cyberspace* – nell'interesse della stessa persona cui si riferiscono, oltre che dei soggetti e degli enti che li trattano, e spesso della stessa collettività, da regolare sulla base del "consenso" o comunque - secondo il modello europeo - di dettagliate disposizioni affidate alla vigilanza ed aggiornamento costanti di un'Autorità garante, munita di penetranti poteri di intervento, autorizzazione, indagine, nonché sanzionatori [6].

L'importanza di questo bene giuridico – nei suoi molteplici aspetti – e la fragilità cui è esposto, rispetto ad offese dalle quali il titolare non può autonomamente difendersi in modo adeguato, per la forte sproporzione di risorse e di possibilità tecnologiche di controllo e autotutela, rende necessario un efficace intervento pubblico di protezione che, in mancanza di sufficiente capacità preventiva di sanzioni soltanto civilistiche e amministrative, da valutare anche dal puto di vista degli strumenti di ricerca e raccolta delle prove, deve necessariamente includere anche misure penali.

---

[2] Cfr. Dir. 2012/29/UE del Parlamento Europeo e del Consiglio del 25.10.2012.

[3] Sull'individuazione della "riservatezza informatica" quale nuovo bene giuridico, distinto dalla più generale riservatezza delle comunicazioni nonché dalla *privacy* strettamente intesa, sia consentito rinviare a PICOTTI, voce *Reati informatici*, cit., 20; nella giurisprudenza fondamentale è la sentenza della Corte cost. tedesca sui limiti e le condizioni di ammissibilità delle c.d. perquisizioni in rete (*online-Durchsuchung*): cfr. Bundesverfassungsgericht, 27.02.2008,379/2007-595/2007, su cui si veda in italiano il commento di FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online-Durchsuchung, in *Riv. trim. dir. pen. ec.*, 2009, 695 s.

[4] Si rinvia sempre allo storico contributo di WARREN, BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, 15.12.1890.

[5] Per il riconoscimento della nascita di tale "nuovo" diritto come diritto al controllo su propri dati e la loro circolazione, cfr. nella dottrina italiana i fondamentali contributi di RODOTÀ, a partire da *Elaboratori elettronici e controllo sociale*, Bologna, 1973 fino ad *Intervista su privacy e libertà*, Bari, 2005 ed altri successivi; nella dottrina penale PATRONO, *Privacy e vita privata*, in *Enc. Dir.*, XXXV, Milano, 1985, 557 s.; volendo, per la distinzione dai diritti relativi al trattamento di dati personali, PICOTTI, *Tutela dei dati personali e tutela della persona*, in CAMMELLI, GUERRA (cur.), *Informazione e funzione amministrativa*, Rimini, 1997, 297 s.

[6] Basti qui il richiamo allo specifico contenuto dell'art. 8 della Carta di Nizza.

3.3. *La sicurezza informatica.*

Non meno importante è il nuovo bene giuridico della "sicurezza informatica", che non è soltanto *strumentale* alla protezione degli altri interessi e diritti della persona meritevoli di tutela nel *Cyberspace* - a cominciare dalla riservatezza informatica e dalla *privacy*, appena menzionate - ma è a sua volta meritevole e bisognoso di un'*autonoma* efficace protezione giuridica, compresa quella penale, in quanto svolge una funzione di *garanzia* "preventiva" di tutti gli altri interessi e diritti che emergono e si esercitano nello "spazio" cibernetico, al punto da divenire, a certe condizioni, "indisponibile" per gli stessi titolari dei sistemi informatici, perché *collettivamente* condiviso, nella dimensione globale e di stretta interdipendenza che hanno i rapporti e le attività in Rete[7].

Infatti, una vulnerabilità nella protezione di qualsivoglia sistema, inestricabilmente connesso con gli altri, si riverbera necessariamente – quale smagliatura della Rete - sulla sicurezza di tutti.

Proprio questa dimensione sovraindividuale e di stretta interdipendenza, che assumono dunque sia la sicurezza che la riservatezza, al pari di altri beni e diritti nel *Cyberspace*, dimostra altresì l'importanza crescente del ruolo degli *Internet Service Providers* (ISP), che in relazione ai diversi servizi ed alle plurime attività che vi si svolgono, diventano necessariamente anche centri d'imputazione di responsabilità - civili, penali ed amministrative - il cui fondamento positivo e la cui delimitazione precisa pongono rilevanti problemi giuridici (oltre che di politica del diritto e di implementazione pratica), certamente non risolti dalla vetusta regolamentazione, d'ispirazione sopranazionale, risalente all'originario modello delineato dal *Millennium Copyright Act* statunitense del 1997 e dalla Direttiva CE 2000/31 sul commercio elettronico, che in parte lo ha ricalcato, sulla cui inadeguatezza, rispetto all'impressionante evoluzione successiva, occorrerà specificamente ritornare.

4. I singoli reati

4.1. *L'accesso abusivo* – La prima fattispecie paradigmatica che merita attenzione per la tipizzazione di condotte inconcepibili al di fuori del contesto informatico è quella che punisce l'accesso abusivo ad un sistema informatico o telematico, cui fanno da contorno le fattispecie prodromiche di cui agli artt. 615-*quater* (*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*) e 615-*quinquies* c.p. (*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*).

Si tratta di un delitto a sua volta prodromico rispetto a molteplici altre condotte delittuose nel *Cyberspace*, non a caso collocato al primo posto della lista dei reati da incriminare sia nella Convenzione *Cybercrime* del 2001, sia negli strumenti di armonizzazione europei del 2005 e del 2013, laddove nelle risalenti Raccomandazioni del Consiglio d'Europa del 1989 aveva una posizione secondaria, tanto da essere stato collocato soltanto alla lettera e) della c.d. lista obbligatoria e da non aver neppure trovato ingresso in importanti ordinamenti giuridici, quale quello della Repubblica federale tedesca, che non lo aveva previsto fra i reati informatici introdotti nel codice penale dalla c.d. seconda legge contro la criminalità economica del 1986 (2. WiKG)[8].

In effetti è stata la possibilità di commissione in rete - "da remoto" - che lo ha reso particolarmente temibile dopo l'apertura al pubblico di Internet, in cui trova frequente realizzazione in molteplici contesti e con svariate modalità e scopi.

La formulazione del nostro codice riecheggia le condotte incriminate dal delitto di violazione di domicilio di cui all'art. 614 c.p., per la dichiarata analogia che il legislatore del 1993 ravvisava fra "domicilio informatico" e domicilio fisico tradizionalmente inteso, la cui tutela sarebbe parimenti fondata costituzionalmente sull'art. 14 Cost. Per cui non solo presenta analoghi limiti edittali di pena, ma si articola altresì nelle due condotte dell'"introduzione" abusiva ed – a differenza di quanto

[7] PICOTTI, *Sicurezza, informatica e diritto penale,* in DONINI, PAVARINI (cur.), *Sicurezza e diritto penale,* Bologna 2011, 217 s.

[8] Per un'analitica ricostruzione in lingua italiana sia consentito rinviare PICOTTI, *Studi*, cit., 33 s.

previsto a livello internazionale e nella maggioranza degli altri ordinamenti – anche del "mantenimento" (dopo un accesso legittimo) contro la volontà del titolare dello *jus excludendi*.

La diversità strutturale di queste due ipotesi è però ben presto emersa, sia con riferimento alla necessità di definire la condotta di "introduzione" nel sistema, ovviamente alla stregua della tecnologia informatica, con non poca difficoltà di fissare il correlativo *tempus* e soprattutto *locus commissi deliciti*; sia con riguardo alla specifica delimitazione della condotta di "mantenimento" penalmente rilevante, logicamente successiva ad un'introduzione autorizzata, che resterebbe altrimenti assorbita nell'accesso abusivo.

Le Sezioni unite della Corte di Cassazione sono già state chiamate in tre occasioni a definire un orientamento coerente su tali questioni, riuscendovi solo in parte, di fronte alle perduranti incertezze ed ai contrasti giurisprudenziali.

Quanto al primo profilo, la sentenza del 2015 (ric. Rocco) ha individuato il *luogo di commissione* in quello in cui si trova l'autore che opera l'accesso, introducendosi o mantenendosi così nel sistema, non invece in quello del server del sistema aggredito (nella fattispecie: il terminale periferico di accesso in Napoli, anziché il server centrale della motorizzazione civile in Roma), data l'affermata "unitarietà" ed "immaterialità" della stessa nozione di sistema informatico[9]. Ma restano forti perplessità concettuali e difficoltà di applicazione, acuite dai sempre più frequenti casi di ricorso a dispositivi mobili, che aumentano gli ostacoli per le attività investigative e per l'esigenza di prossimità alla prova, non agevolando l'azione di tutela delle vittime.

In realtà il *momento* consumativo dell'"introduzione" (che non coincide esattamente con il concetto prodromico di "accesso" utilizzato invece nella rubrica e nella terminologia delle fonti sovranazionali) può ravvisarsi solo quando e laddove si sia esplicato un effettivo controllo *informatico* delle credenziali od azioni d'accesso, che in rete avviene tramite *connessione* telematica fra terminale e server, presso il quale ultimo soltanto può dirsi precisamente *perfezionata* l'"introduzione", come fase finale della procedura, distinta dalla previa mera "immissione" dei dati, che ancora non implica alcun effettivo *trattamento* automatizzato operato dal sistema *nell'ambito* degli "spazi informatici" di cui è titolare la vittima.

Quanto alla condotta di "mantenimento", essa può assumere rilevanza penale solo quando e laddove infranga – in un momento *successivo* all'"introduzione" - le regole e le disposizioni dell'avente diritto, circa le "azioni" che si possono porre in essere *in* detti spazi informatici. Per cui *a fortiori*, sotto il profilo della tecnologia informatica, quest'attività si svolge nel luogo in cui è posto il server (ivi comprendendosi il *cloud* e qualsiasi altro dispositivo o memoria, in cui si collochino fisicamente gli spazi informatici, disponibili esclusivamente in capo al loro titolare), non certo nel luogo in cui è posto invece il terminale periferico da cui vengono soltanto immessi i dati.

Come si è premesso (cfr. *supra* § 2), non è infatti il mero segmento dell'azione umana materialmente intesa (quella dell'operatore che agisce al terminale digitando dati), che può integrare il "fatto" tipico, concretamente *offensivo* degli interessi giuridici protetti, ma solo la sua connessione con il trattamento *automatico* che ne consegue e che la "sostituisce" nelle ulteriori decisive fasi, realizzate in base al *software* dal sistema informatico, il quale solo idealmente e fittiziamente può però ridursi ad un'unitaria ed in tal modo indistinta realtà "immateriale", come ipotizza la Suprema Corte, non coincidendo affatto con l'intero insieme dei dispositivi connessi in Rete, che finirebbe per confondersi con l'indistinto *Cyberspace*.

Quanto al secondo profilo, concernente i requisiti più specifici della condotta di "mantenimento" illecito, una prima sentenza delle Sezioni unite del 2011 (ric. Cusani) ha stabilito che è penalmente rilevante la condotta del soggetto che, pur legittimato all'accesso, violi *oggettivamente* le condizioni ed i limiti imposti dal titolare per disciplinarlo, anche con misure organizzative o prassi aziendali, non essendo invece determinanti gli scopi e le finalità *soggettive* dell'autore che si "mantenga" nel sistema in contrasto con quelle disposizioni (nella specie un pubblico ufficiale, utilizzando le proprie

[9] Cass., Sez. un., 26.3.2015 (dep. 24.4.2015), Rocco, n. 17325, in *Dir. pen. proc.*, 2015, 1296 s., con nota critica di FLOR, *I limiti del principio di territorialità nel "cyberspace". Rilievi critici alla luce del recente orientamento delle sezioni unite*.

credenziali di autenticazione e di accesso, si era introdotto nel sistema informatico S.D.I., protetto da misure di sicurezza, operando poi per finalità diverse da quelle istituzionali)[10].

Tuttavia una più recente sentenza del 2017 (ric. Savarese) ha precisato – per vero con riguardo all'ipotesi aggravata di cui al comma 2, n. 1 dell'art. 615-*ter* c.p., che fa espresso riferimento al pubblico ufficiale od incaricato di pubblico servizio, che commetta il fatto "con *abuso* dei poteri o *violazione* dei doveri inerenti alla funzione od al servizio" (corsivi aggiunti) – che il delitto è commesso anche quando l'agente "pur non violando le prescrizioni formali impartite dal titolare" del sistema per delimitarne l'accesso, vi acceda o vi si mantenga "per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita" (nella specie un cancelliere accedendo al Registro informatico delle notizie di reato REGE aveva visionato il fascicolo processuale di un conoscente)[11].

In tal modo, più che dar rilievo alle finalità soggettive dell'agente, e dunque senza affatto entrare in contrasto per tale aspetto con la precedente sentenza Cusani, come da taluno sostenuto, la Corte di legittimità ha sovrapposto il concetto di "abusività" - quale violazione delle specifiche regole di gestione del sistema informatico - all'"abuso" o, meglio, allo "sviamento" dei poteri e doveri *pubblicistici* dell'agente, in questi termini qualificato ai fini dell'applicazione dell'aggravante. Ma l'esito non sembra criticabile, se si considera che viene utilizzato un criterio pur sempre oggettivo e di natura normativa, analogo a quello che traspare dalla struttura del delitto di rivelazione o utilizzazione di segreti d'ufficio, di cui all'art. 326 c.p., in cui parimenti converge la tutela del bene giuridico "finale" (del buon andamento e dell'imparzialità della pubblica amministrazione) con quella del bene giuridico "strumentale" della segretezza delle notizie conosciute per ragioni d'ufficio. E non diversa è la natura delle "ragioni d'ufficio" per cui è conferita e, dunque, necessariamente *limitata* – con "regole" di condotta di carattere *anche* generale, non solo tecniche - la facoltà d'accesso del pubblico ufficiale al sistema informatico dell'amministrazione cui è addetto, che rappresentano dunque un elemento normativo extrapenale della fattispecie in esame, non necessariamente coincidente con disposizioni di natura tecnico-informatica che specificamente debbano disciplinare l'accesso al sistema stesso ed il suo utilizzo, tanto da poter e dover essere rispettate anche in assenza di queste ultime.

In definitiva, la norma incrimina ogni *oggettiva* violazione dell'"esclusiva disponibilità", in capo al titolare, degli *spazi* informatici cui ha diritto (*jus excludendi alios*), in quanto instaura un *rapporto conflittuale* apprezzabile con riguardo non solo alle procedure informatiche che *tecnicamente* abilitano e legittimano l'"introduzione" e l'utilizzo del sistema, ma anche con riguardo alle regole e disposizioni generali, pur se non strettamente informatiche, aventi contenuto precettivo, poste dal titolare del sistema od a lui riferibili anche per regolare il successivo "mantenimento" in tali spazi, che è da qualificare *contra jus* se in *contrasto* con la sua "volontà". Questa non è naturalmente da intendere in termini psicologici o soggettivi, essendo del resto ben difficilmente concepibile e riconoscibile in capo ad un ente o ad un'amministrazione, quanto sul piano *oggettivo* delle regole e disposizioni con cui viene ad esternarsi, che sono anche indirettamente integrate dalla disciplina delle competenze e delle attività d'ufficio, come di regola avviene nel caso di organizzazioni complesse, sia private che pubbliche, la cui violazione integra il requisito dell'"abuso dei poteri o della violazione dei doveri (richiesto dall'aggravante di cui al comma 2 dell'art. 615-*ter* c.p.), costituente un elemento normativo extrapenale, che completa la tipizzazione del "fatto" oggettivo costitutivo del reato.

---

[10] Cass. Sez. un. 27.10.2011 (7.2.2012) Casani, n. 4694, *ex multis* in www.penalecontemporaneo.it (2.5.2012), con nota di FLOR, *Verso una rivalutazione dell'art. 615* ter *c.p.?* a commento vedi anche SALVADORI, *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615*-ter *c.p.*, in *Riv.trim.dir.pen.ec.*, 2012, 369 s.

[11] Cass. Sez. un. 18.5.2017 (8.9.2017) Savarese n. 41210, in www.penalecontemporaneo.it (3.10.2017), con nota di BERTOLISI, *Accesso abusivo a un sistema informatico: è reato la condotta del pubblico ufficiale commessa con c.d. sviamento di potere*; cfr. anche FLOR, *La condotta del pubblico ufficiale fra violazione della* voluntas domini*, "abuso" dei profili autorizzativi e "sviamento di potere"*, in *Dir.pen.proc.* 2018, 506 s.

4.2. *I reati c.d. prodromici o preparatori.*

4.2.1. *La diffusione e detenzione abusive di dispositivi d'accesso (art. 615*-quater *c.p.)* - La previsione del delitto di «*detenzione e diffusione abusiva di codici di acceso a sistemi informatici o telematici*» (art. 615-*quater* c.p.) ha costituito una novità nel panorama europeo, dal momento che il legislatore del 1993 ha anticipato le scelte politiche sovranazionali, ed in specie del Consiglio d'Europa (art. 6 Convenzione *Cybercrime*) e dell'Unione europea (art. 7 Direttiva 2013/40/UE), che sollecitano gli Stati a punire il c.d. abuso di dispositivi (*misuse of device*).

La *ratio* della norma incriminatrice è di tutelare, in via anticipata, il bene giuridico della *riservatezza informatica*, e, in via mediata, quello della *sicurezza informatica* (su cui v. *supra* § 3) incriminando condotte prodromiche o preparatorie alla commissione di più gravi reati informatici (accesso abusivo ad un sistema informatico, danneggiamenti informatici, intercettazioni e frodi informatiche, ecc.), consistenti nel procurarsi e/o mettere in circolazione mezzi idonei a facilitare le intrusioni in sistemi altrui. In tal senso è da condividere la scelta legislativa di collocare la norma in esame subito dopo quella che incrimina l'accesso abusivo ad un sistema informatico o telematico. Solleva, però, notevoli perplessità, l'inquadramento sistematico della menzionata disposizione nella sezione IV, tra i delitti contro la inviolabilità del domicilio, del titolo XII del libro II del codice penale, in quanto (al pari del delitto d'accesso abusivo) i beni giuridici anticipatamente protetti sono diversi e differenziati.

Due sono le tipologie di condotte previste dalla norma incriminatrice. Da un lato si puniscono i comportamenti non autorizzati che consistono nel "far entrare" nella *propria* sfera di signoria parole chiave (*password*), codici di accesso ovvero altri mezzi (ad es. *software* o dispositivi tecnici) idonei a consentire l'accesso ad un sistema informatico altrui, protetto da misure di sicurezza («*si procura*» o «*riproduce*»). Dall'altro vengono sanzionate condotte che si sostanziano nel "mettere a disposizione" *di terzi* i menzionati "oggetti" materiali («*procura ad altri*» «*diffonde*», «*comunica*» ovvero «*consegna*»).

Il legislatore ha altresì punito la condotta, ulteriormente prodromica, del «*fornire*» istruzioni o indicazioni idonee a far entrare nella sfera di signoria altrui ovvero ad agevolare a terzi il conseguimento di mezzi o dispositivi idonei ad accedere abusivamente ad un sistema informatico. L'impiego di questa "clausola di chiusura" permette di ricondurre nell'alveo dell'art. 615-*quater* c.p. i comportamenti che consistono nel procurare o nel mettere a disposizione, mediante qualsiasi modalità, a soggetti determinati le informazioni o le tecniche atte a introdursi abusivamente in un sistema informatico.

Contrariamente a quanto indicato nella rubrica dell'art. 615-*quater* c.p., il precetto non punisce invece la mera «*detenzione*» di codici di accesso[12].

Qualche perplessità sorge rispetto alla nota di "abusività" che deve caratterizzare le condotte tipiche di cui all'art. 615-*quater* c.p. Secondo un orientamento dottrinale, mediante la previsione dell'avverbio «*abusivamente*» il legislatore avrebbe voluto richiamare il giudice al suo dovere di esaminare con particolare attenzione l'assenza di cause di giustificazione[13]. Va detto, tuttavia, che la previsione del menzionato avverbio arricchisce la tipizzazione del fatto costitutivo di reato, qualificando la condotta come "abusiva" in termini oggettivi, prima ancora che soggettivi[14]. Non si tratta dunque di constatare la mera assenza di cause di giustificazione, ma di riconoscere che si tratta di una clausola di *antigiuridicità speciale*, mediante la quale il legislatore ha opportunamente inteso rinviare a regole extrapenali di comportamento, desumibili anche dal contesto professionale, sociale, lavorativo, ecc., nel quale il soggetto agente opera, di cui è richiesta la violazione per circoscrivere la sfera di rilevanza penale[15].

---

[12] Di diverso parere MANTOVANI F., *Diritto penale, P. Sp.*, I, Padova, p. 580, nota 93, secondo cui la detenzione è il presupposto comune di tutte le condotte richiamate dal precetto.

[13] In questi termini v. già MARINI, *Delitti contro la persona*, Torino, II ed., 1996, 390-391; MANTOVANI F., *Diritto penale*, *P. Sp.*, I, cit., 575.

[14] Il soggetto agente dovrà essere "consapevole" altresì dell'abusività della condotta, dal momento che nell'oggetto del dolo rientrano anche gli elementi normativi che concorrono a dare "materia" al precetto.

[15] Cfr. PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. dell'Internet*, n. 2, 2005, 189 ss., 197.

L'oggetto materiale del reato è costituito da «*codici, parole chiave o altri mezzi idonei*» ad accedere ad un sistema informatico o telematico ovvero da «*indicazioni o istruzioni idonee*» al predetto scopo. Mediante la locuzione «*altri mezzi idonei*», che si configura quale "clausola di chiusura" estremamente elastica, capace di ricomprendere gli strumenti tecnologici (anche *software*) non ancora scoperti, il legislatore ha voluto sanzionare non solo i dispositivi multifunzionali o multiscopo, che consentono di aggirare le misure di sicurezza poste a protezione di un sistema informatico e di accedere ai dati ed ai programmi in esso contenuti (c.d. *hacking tools*), ma anche qualsiasi dispositivo o mezzo fisico, che permetta di introdursi in un sistema[16].

Il delitto è punibile soltanto se viene integrato il dolo specifico richiesto, dal momento che le condotte descritte appaiono altrimenti "neutre", consistendo nell'esercitare un potere di signoria ovvero nel mettere a disposizione di terzi mezzi idonei ad accedere ad un sistema informatico altrui: per cui per avere rilievo penale devono essere sorrette dal *fine specifico* di «*procurare a sé o ad altri un profitto*» ovvero «*di arrecare ad altri un danno*». Con tale opportuna previsione, il legislatore ha voluto delimitare la punibilità ai comportamenti, prodromici e preparatori alla commissione di un reato informatico, in quanto commessi dall'agente per realizzare un interesse (profitto proprio o di altri ovvero danno altrui) che si ponga in *oggettivo conflitto* con gli interessi giuridici protetti dalla norma incriminatrice (alla riservatezza informatica ed alla esclusiva disponibilità ed integrità dei dati e dei sistemi informatici), facenti capo a terzi.

4.2.2. *La diffusione e detenzione abusive di* malware *(art. 615-*quinquies *c.p.)* - Anche la previsione del delitto di «*diffusione di apparecchiature dirette a danneggiare un sistema informatico o telematico*» di cui all' art. 615-*quinquies* c.p. ha costituito, al pari di quella di cui all'art. 615-*quater* c.p., una novità nel panorama europeo, dal momento che il legislatore del 1993 ha anticipato le scelte politico-criminali sovranazionali, ed in specie del Consiglio d'Europa (art. 6 Convenzione *Cybercrime*) e dell'Unione europea (art. 7 direttiva 2013/40/UE), che sollecitano gli Stati a punire il già menzionato "abuso di dispositivi" (*misuse of device*) anche sotto il profilo delle condotte volte a favorire la circolazione o l'utilizzo di apparecchiature o programmi idonei a realizzare i più gravi reati di *danneggiamento* di dati o di sistemi informatici.

L'art. 615-*quinquies* c.p. punisce in effetti un ampio ventaglio di condotte preparatorie alla commissione dei reati di danneggiamento di dati, di informazioni o programmi informatici (artt. 635-*bis* e 635-*ter* c.p.) ovvero di sistemi informatici o telematici (artt. 635-*quater* e 635-*quinquies* c.p.).

A differenza di quanto previsto dall'art. 615-*quater* c.p., il legislatore del 1993 aveva originariamente punito soltanto le condotte volte a "far entrare" i c.d. *malware* nella sfera altrui («*diffonde*», «*comunica*» ovvero «*consegna*»). Con la L. 48/2008, di ratifica ed esecuzione della Convenzione *Cybercrime*, è stata modificata la criticabile formulazione della norma in esame, con il condivisibile proposito di adeguarla agli *standard* sovranazionali. L'opportuna estensione del novero delle condotte penalmente rilevanti anche a quelle volte a far entrare i predetti *malware* nella sfera di signoria dello stesso agente («*si procura*», «*produce*», «*riproduce*» o «*importa*») ha reso la formulazione della previsione legale omogenea rispetto a quella dell'art. 615-*quater* c.p.

A seguito delle modifiche introdotte dalla menzionata L. 48/2008, le condotte tipiche devono avere ad oggetto «*apparecchiature, dispositivi o programmi informatici*». Non è richiesto, però, come stabilito dall'art. 6 della Convenzione *Cybercrime*, che questi ultimi siano «*principalmente adattati o disegnati*» per commettere un reato informatico contro la esclusiva disponibilità ed integrità di dati o di sistemi informatici.

Mancando anzi ogni riferimento all'*intrinseca* dannosità o pericolosità dei "dispositivi" che devono essere oggetto delle condotte - di per sé "neutre" - di *procurarsi, produrre, diffondere, importare, distribuire* o *cedere*, il contenuto d'offesa oggetto della norma incriminatrice viene in modo discutibile ricavato esclusivamente sul *fine illecito* che deve sorreggere il fatto-base. Ma in

[16] Sulle peculiari caratteristiche dei *software* a "duplice uso" e le tecniche adottate nel diritto penale italiano e comparato per incriminarne l'impiego illecito v. SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei* dual-use software, in *Riv. it. dir. proc. pen*., 2017, 747 s.

questo modo si è tipizzata una condotta altrimenti priva di autonoma offensività oggettiva. Il delitto è in effetti punibile solo a titolo di dolo specifico, dal momento che le condotte "neutre" che si sostanziano nell'esercizio di una signoria ovvero nel mettere a disposizione di terzi apparecchiature, dispositivi o programmi informatici, rispetto ai quali, come si è visto, non viene richiesta alcuna qualificazione intrinseca di dannosità (enunciata peraltro nella rubrica della disposizione), devono essere sorrette dal *fine specifico* di *danneggiare* illecitamente un sistema informatico o telematico oppure i dati in essi contenuti od ancora di *favorire l'interruzione*, totale o parziale, o *l'alterazione del funzionamento* di un sistema informatico o telematico[17].

Dal punto di vista della struttura normativa, l'art. 615-*quater* c.p. si configura dunque, al pari dell'art. 615-*quater* c.p., come un reato di pericolo indiretto, che anticipa notevolmente la tutela del bene giuridico della sicurezza (e della riservatezza) informatica. Pertanto è escludere la punibilità del tentativo di detti reati.

4.3. *La corrispondenza informatica* – In altre ipotesi, a differenza di quanto si è visto per i delitti di accesso abusivo ed i reati prodromici rispetto alla tutela della riservatezza e della sicurezza informatiche, il legislatore non ha introdotto fattispecie incriminatrici integralmente nuove, ma si è limitato a ridefinire o aggiungere oggetti passivi o materiali "nuovi", ovvero talune "nuove" modalità di condotta, alla tipizzazione di fattispecie comuni già esistenti, secondo un criterio di "analogia" che per il resto rinvia direttamente ad esse o ne riproduce gli elementi essenziali (come è ben esemplificato dal delitto di danneggiamento di dati e sistemi informatici, di cui all'art. 635-*bis* c.p., introdotto nel 1993 e poi riformulato, con la previsione di ben quattro distinte fattispecie, nel 2008).

Di questa tecnica di tipizzazione è emblematica la tutela della corrispondenza informatica.

Con il comma 4 aggiunto all'art. 616 c.p., il legislatore ha stabilito fin dal 1993 che: "Agli effetti delle disposizioni di questa sezione [V del capo III del titolo XII, dedicata all'inviolabilità di segreti] per corrispondenza si intende quella epistolare, telegrafica, telefonica, *informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza*" (corsivi aggiunti). Dunque il legislatore non ha fatto ricorso ad una definizione *ad hoc* dell'oggetto materiale delle condotte punibili (come si era verificato invece a proposito dei delitti di falsità in documenti informatici di cui all'art. 491-*bis* c.p., quale introdotto nel 1993, poi riformulato nel 2008), ma ha soltanto esteso l'applicabilità di – apparentemente - *tutte* le fattispecie in materia di corrispondenza alle nuove forme di "comunicazione", addirittura chiudendo l'elencazione con una formula aperta all'evoluzione tecnologica futura ("*ogni altra forma* …"), che rischia, per la sua indeterminatezza, di consentire estensioni analogiche *in malam partem*, evitabili solo circoscrivendo concettualmente il *genus* cui possano ricondursi le varie *species*, comprese quelle non (ancora) espressamente denominate o disciplinate dal legislatore[18]. Operazione non semplice, vista la peculiarità strutturale e soprattutto varietà delle nuove forme telematiche di comunicazione, che coinvolgono "attivamente" una possibile pluralità di destinatari e ne consentono la circolazione, simultanea o meno, nell'ambito di gruppi, reti sociali, *chat* aperte, ecc., di estensione assai variabile e talora persino "indeterminata".

Inoltre, appare spesso problematica la distinzione fra comunicazioni informatiche e telematiche che devono ricadere sotto la disciplina (meno severa) della "corrispondenza" e quelle invece da ricondurre alla disciplina più rigorosa delle "intercettazioni", parallelamente estesa a quelle informatiche e telematiche (nuovi artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p., parimenti introdotti dalla L. 547 del 1993). Distinzione che ha rilevanti ricadute non solo sul piano dei requisiti di tipicità dei relativi reati e delle pene applicabili, ma anche in campo processuale, con specifico

[17] Si tratta dunque di reati composti di un altro reato, che costituisce l'oggetto del dolo specifico che deve sorreggere il fatto-base. Sulla peculiare categoria del "reato-elemento del reato" v. i rilievi di MORGANTE G., *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale*, Torino, 2013, in specie p. 10 ss., p. 58 ss.

[18] Cfr. PECORELLA, *Il diritto penale cit.*, 292 s.; volendo anche PICOTTI, *Commento art. 5 L.23.12.1993, n. 547 (art. 616, comma 4 c.p.)*, in *Leg. pen.*, 1996, 109 s., in specie 115 s.

riguardo alla diversa disciplina dei sequestri, da un lato (in specie *ex* artt. 254, 254-*bis* e segg. c.p.p.), e delle intercettazioni, dall'altro (art. 266-*bis* c.p.p.)[19].

Anche in tali ipotesi, dunque, si palesa la necessità di rileggere le diverse fattispecie penali alla luce dei caratteri specifici delle TIC, che vanno ad incidere – a seconda delle varie procedure *automatizzate* di trasmissione, memorizzazione, messa a disposizione in rete di dati di ogni genere, sia scritti che vocali o visivi, e ad un numero limitato ovvero indiscriminato di destinatari od utenti, ecc. - sulla struttura stessa delle modalità di "comunicazione" fra persone, e dunque sulle varie condotte punibili di "presa di cognizione", "sottrazione", "distrazione", "distruzione", "soppressione", "rivelazione", richiedenti (*ex* art. 616, commi 1 e 2 c.p.) l'ulteriore individuazione dei requisiti per definire una "corrispondenza informatica" come "chiusa" anziché "aperta"[20]. Inevitabili sono le ripercussioni anche sulla definizione del bene o dei beni giuridici tutelati, che non possono circoscriversi alla dimensione meramente "privata" della relazione comunicativa fra un mittente ed uno o più destinatari comunque ben determinati, che è alla base del "segreto" epistolare, lasciata perciò dal legislatore alla piena disponibilità del titolare del relativo diritto, anche di querela, *ex* art. 616 comma 3, c.p., dato che ora può venire invece in rilievo anche la generale sicurezza e correttezza, ed addirittura "veridicità", oltre che riservatezza, delle varie forme di scambio e circolazione nel *web*, capaci di coinvolgere contemporaneamente od a catena pluralità assai ampie o indeterminate di utenti, con conseguenze lesive che possono andare ben al di là della mera offesa al bene individuale del singolo "segreto" epistolare.

4.4. *Le "altre comunicazioni" a distanza* – La norma "di chiusura" della sezione V, di cui all'art. 623-*bis* c.p., già introdotto nella sua formulazione originaria nel 1974 per contrastare le intrusioni nella riservatezza delle "comunicazioni e conversazioni telegrafiche [e] telefoniche", estendendo ad esse l'applicazione di tutte le disposizioni contenute nella sezione predetta[21], comprende – dopo la novella del 1993 - anche quelle "informatiche o telematiche" e stabilisce che *tutte* tali disposizioni si applichino altresì "a qualunque altra trasmissione a distanza di suoni, immagini od altri dati".

La norma opera però così una criticabile apertura a possibili estensioni analogiche, in quanto risulta difficile delimitare *a priori* i caratteri identificativi della categoria, come già si è visto a proposito della simile clausola che chiude anche la definizione di "corrispondenza". Né si è avuta fino a d oggi una concreta operatività di tale clausola aggiuntiva, mentre paradossalmente proprio quella aggiunta nel 1974 aveva fatto emergere lacune di tutela in relazione all'intercettazione di comunicazioni radio riservate fra le forze di polizia, perché non avrebbe consentito di ricomprendervi quelle mediante c.d. "onde guidate".

In altri termini, si dimostra che *l'horror vacui* non può essere un criterio razionale di guida per il legislatore nella formulazione della disciplina penale diretta a contrastare i fenomeni criminosi nascenti dall'utilizzo delle nuove tecnologie, occorrendo piuttosto che vi sia sempre, alla base delle scelte di politica criminale e delle correlate formulazioni normative, un'attenta analisi e conoscenza degli stessi fenomeni, sia sul paino criminologico, sia su quello più specificamente tecnico.

4.5. *Il "furto d'identità digitale" fra tutela del patrimonio e tutela della persona* - L'art. 9, co. I, lett. a), della legge, 15 ottobre 2013, n. 119, che ha convertito in legge, con modificazioni, il decreto-

[19] In argomento si veda PECORELLA, *Il diritto penale*, cit., 302 s.

[20] Il recente D.Lgs. n. 101 del 2018 contenente disposizioni di adeguamento del Codice privacy al GDPR dell'Unione europea 2016/679, al nuovo comma 1-bis dell'art. 121 relativo ai "servizi interessati" contiene alla lettera m) la seguente definizione di "posta elettronica": "messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza". Seppur non direttamente traslabile nella disciplina penale in esame, la definizione è rilevante perché tipizza il carattere comunicativo fra persone del messaggio, che è destinato alla "conoscenza" del suo contenuto da parte del ricevente, avvenuta la quale perde il suo requisito distintivo rispetto ad altre categorie di dati.

[21] Sulla finalità di tutela della riservatezza dalle intrusioni consentite dai nuovi strumenti tecnici di allora, quali microspie e teleobiettivi, perseguita dalla L. 8.4.1974, n. 98, si veda l'importante contributo di BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv.it.dir.proc.pen.*, 1967, 1079 s., ora in *Scritti diritto penale*, II, Tomo I, Milano, 1997, 2289 s.

legge 14 agosto 2013, n. 93, ("recante disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché' in tema di protezione civile e di commissariamento delle province") ha inserito nell'art. 640-*ter* c.p. ("frode informatica"), un nuovo comma, che sanziona la frode informatica commessa mediante sostituzione (*furto o indebito utilizzo*) *"dell'identità digitale in danno di uno o più soggetti"*.
Sul piano della collocazione sistematica, una parte della dottrina[22] ritiene si tratti di una circostanza aggravante della frode informatica, argomentando sul tenore della disposizione, che utilizza i termini "*se il fatto è commesso con*", anziché ridescriverlo o perlomeno usare la locuzione: "se il fatto *consiste* in", rinviando necessariamente al contenuto tipizzato nell'ipotesi base di cui al co. 1 dell'art. 640-*ter*.[23]

4.5.1. *Formulazione tecnica delle "modalità di realizzazione" delle condotte tipiche*
In verità sollevano maggiori dubbi le questioni relative alla formulazione tecnica della fattispecie e all'assenza di una definizione di "identità digitale" che possa essere rilevante almeno agli effetti della legge penale.
Sembra opportuno evidenziare che in sede di conversione del decreto legge, il Parlamento, anziché adottare l'originaria locuzione «*se il fatto è commesso con sostituzione dell'identità digitale in danno di uno o più soggetti*», ha optato per quella: «*furto o indebito utilizzo*». Pur ritenendo apprezzabile la modifica del termine originario apparentemente troppo ambiguo[24], l'espressione "furto" d'identità digitale sembra richiamare (impropriamente) le condotte di sottrazione e impossessamento previste dall'art. 624 c.p., che sono tecnicamente riferite ad un oggetto fisico-materiale, espresso dal termine "cosa".
L'identità digitale, però, anche se non definita normativamente, è chiaramente da intendersi quale entità immateriale[25] insuscettibile di sottrazione ed impossessamento. Anche se fosse "incorporata" in un supporto informatico, sarebbe quest'ultimo a rappresentare l'oggetto – la *res* - del "furto"[26].
Proprio le difficoltà sorte nel definire l'"acquisizione abusiva" dell'identità digitale, ha portato il legislatore a fare riferimento, in settori *extra* penalistici, alla nozione di «*impersonificazione*», definita dall'art. 30-*bis* del D. lgs. 141/2010[27]. Anch'essa, però, ammesso che possa costituire un utile parametro ermeneutico di ordine sistematico, appare inidonea a chiarire la distinzione, introdotta dal legislatore penale, fra "furto" e "utilizzo"[28].

---

[22] Cfr. MALGIERI, *La nuova fattispecie di "indebito utlizzo d'identità digitale": un problema interpretativo*, in *Dir. pen. cont.*, fasc. 2, 2015, 143 ss.; ID., Il furto di "identità digitale": una tutela patrimoniale della personalità, in FALCINELLI, FLOR, MARCOLINI (a cura di), *La giustizia penale nella "rete",* Milano, 2015, 37 ss; CRESCIOLI, *La tutela penale dell'identità digitale*, in *Dir. pen. cont.*, 5/2018, 265 ss.

[23] MALGIERI, *La nuova fattispecie*, cit., 145.

[24] In tal senso PISTORELLI, *Relazione Ufficio del Massimario Cassazione*, n. III/01/2013 del 22 agosto 2013, p. 7; CAJANI, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, in *Cass. pen.*, fasc. 3, 2014, 1103.

[25] FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen*., 2007, n. 2-3, 899 ss

[26] Ibidem 910; *contra* FALCINELLI, *Tempi moderni e cultura digitale: il valore patrimoniale dell'identità umana "on line"*, in *Ind. pen.*, 2015, 297 ss. che argomenta sulla necessità di far progredire l'ordinamento penale in base all'evolversi della cultura sociale, anche sganciandosi dai vincoli dell'art. 2 c.p., sicché è possibile considerare l'identità digitale come "cosa mobile" e, dunque, applicare l'art. 624 c.p.

[27] Si tratta del decreto di attuazione della direttiva 2008/48/CE relativa ai contratti di credito ai consumatori, nonche' modifiche del titolo VI del testo unico bancario (decreto legislativo n. 385 del 1993) in merito alla disciplina dei soggetti operanti nel settore finanaziario, degli agenti in attivita' finanziaria e dei mediatori creditizi. (10G0170) (GU n.207 del 4-9- 2010 - Suppl. Ordinario n. 212). L'art. 30 bis, co. 1, prevede che: "Ai fini del presente decreto legislativo per furto d'identita' si intende: a) l'impersonificazione totale: occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto. L'impersonificazione può riguardare l'utilizzo indebito di dati riferibili sia ad un soggetto in vita sia ad un soggetto deceduto; b) l'impersonificazione parziale: occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto, nell'ambito di quelli di cui alla lettera a)".

[28] MALGIERI, *La nuova fattispecie*, cit., 146.

Nemmeno la condotta di "indebito utilizzo" è, infatti, di facile interpretazione[29].
Se l'identità digitale, infatti, costituisce un profilo abilitativo "personale" per la fruizione di (o l'accesso a) determinati spazi informatici o servizi nel *Cyberspace* – vale a dire attraverso i sistemi informatici ed Internet - il suo "utilizzo" appare confondersi con il "trattamento" di *dati personali*, di cui al Codice *privacy* (D.lgs. 196/2003, come modificato dal D.lgs. 101/2018 di attuazione del Regolamento 2016/679/UE, c.d. GDPR).
Infatti, ai sensi dell'art. 4, n. 2, del Regolamento europeo, il "*trattamento*" consiste in qualsiasi operazione od insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali od insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Tale nozione di "trattamento" è riferita però soltanto ai "dati personali". Ed occorre precisare che non sempre è a questi riconducibile l'identità digitale, in quanto essa potrebbe invece costituire una "misura di sicurezza" adottata per la "protezione" dei dati e dei sistemi. Un suo "indebito utilizzo", in tal caso, comporterebbe una – o costituirebbe un'attività prodromica alla – violazione delle misure di sicurezza per l'accesso al sistema o per l'acquisizione di dati e informazioni.
Una parte della dottrina[30] ha ritenuto che potrebbe essere maggiormente coerente con le intenzioni del legislatore richiamare la distinzione tra *unauthorized access* (*accesso* non autorizzato a sistemi altrui / *possesso* non autorizzato di dati altrui) e *unauthorized use* (*uso* non autorizzato di dati altrui lecitamente posseduti)[31] e, dunque, la nozione di «*sostituzione dell'identità digitale*», ne rappresenterebbe generalmente l'effetto o la conseguenza.
Seguendo questa impostazione ermeneutica il «*furto*» dovrebbe essere interpretato alla stregua di un'apprensione illecita dell'identità digitale (o delle sue "componenti" essenziali come, ad es., nome utente e *password*), mentre l'«*indebito utilizzo*» dovrebbe essere inteso quale "uso abusivo" dell'identità digitale[32].

4.5.2. *L'assenza di una definizione di "identità digitale"*

In ogni caso, pur tentando con estrema difficoltà, con riferimento alle condotte tipiche, di fornire soluzioni interpretative nei limiti imposti dal divieto di estensione analogica *in malam partem*, rimane irrisolto il problema definitorio dell' «*identità digitale*», che come già è emerso sopra, potrebbe essere intesa, da un lato, in senso restrittivo, ossia quale "profilo abilitativo" o "credenziali di autenticazione" [33]; dall'altro lato, potrebbe essere ricondotta nell'ambito del più complesso sistema di protezione dei "dati personali".
Una parte della dottrina italiana ha proposto la distinzione fra «identità digitale», «impronta digitale» e «ombra digitale»[34].
L'identità digitale sarebbe «costituita dall'insieme di dati che permettono di ricollegare un documento informatico ad una macchina e quindi al soggetto (fisico o giuridico) che lo possiede»; «essa consta

[29] Ibidem, 144.

[30] Ibidem.

[31] Così MALGIERI, *La nuova fattispecie*, cit., 147; FALCINELLI, *Tempi moderni*, cit., 297 ss.; entrambi rinviano a WASIK, *Crime and the computer*, Oxford, 1991.

[32] Così MALGIERI, *La nuova fattispecie*, cit., pp. 147, 151.

[33] In questo senso FLOR, *Phishing, identity theft*, cit., p. 903. In relazione ai fenomeni criminali come il *phishing*, però, l'Auotre ha distinto *identity abuse, identity theft* e *identity related fraud*. In giurisprudenza vedi Cass. pen., Sez. II, sent. 6 marzo 2013, n. 13475; Cass. pen., Sez. II, sent. 15 marzo 2011, n. 17748.

[34] CIPOLLA, *Social network, furto di identità e reati contro il patrimonio*, in *Giur. Merito*, fasc. 12, 2012, 2675; FALCINELLI, *Tempi moderni*, cit., 308 s.

al minimo dell'*user id* (nome utente) e di una *password*»[35]. Per «impronta digitale» dovrebbe intendersi invece il «complesso delle informazioni fornite consapevolmente da ognuno al sistema telematico, per distinguersi dagli altri»; mentre l'«ombra digitale [sarebbe] composta dall'insieme delle informazioni relative alla vita di ogni individuo, quali i documenti cartacei, fotografici e di altro genere, che derivano dalla frequentazione dell'individuo con l'ambiente (reale e virtuale) che lo circonda»[36].
Un'altra parte della dottrina sembra impiegare il termine "identità digitale" per designare l'«insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore», le quali «di norma, sono protette da un sistema di autenticazione» mediante «parola chiave (*password*), caratteristiche biologiche (iride, impronta digitale, impronta vocale, riconoscimento del volto, ecc.) o attraverso un particolare oggetto (tessera magnetica, *smart card*, ecc.)»[37].
Si tratta di tentativi definitori che, comunque, da un lato, sembrano ruotare attorno alla c.d. fase autenticativa – piuttosto che a quella riconoscitiva - collegata a condotte di "furto" d'identità digitale, in cui il fulcro del disvalore sociale è incentrato sulla acquisizione o sulla sottrazione dei dati riservati, ossia di dati e informazioni di autenticazione o di abilitazione che afferiscono ad un'ampia area di riservatezza del titolare; dall'altro lato, non sembrano poter ovviare all'assenza di una definizione *giuridica* di identità digitale, che sarebbe auspicabile almeno agli "effetti della legge penale", per evitare il rischio di operazioni ermeneutiche eccessivamente late, se non funanmboliche, ovvero eccessivamente restrittive.

4.5.3. *Il bene giuridico protetto*

Un'ulteriore questione che fa emergere l'incriminazione del "furto o indebito utilizzo di identità digitale" è rappresentata dalla sua collocazione sistematica (al comma 3 dell'art. 640-*ter* c.p.), vale a dire quale ipotesi aggravata di frode informatica.
Se si ritiene, infatti, che si tratti di una circostanza aggravante, né il furto, né l'indebito utilizzo di identità digitale possono di per sé assumere rilevanza penale, che è condizionata alla dimensione patrimoniale dell'altrui danno con ingiusto profitto per sé od altri[38].
Appare evidente che la discussione sul bene giuridico protetto dall'incriminazione dell'illegittima acquisizione ed/od abusiva fruizione dell'identità digitale altrui non possa essere ridotta alla sola tutela del patrimonio, di fronte a fenomeni criminosi ormai estremamente diffusi, che vanno ben oltre le truffe e le frodi informatiche commesse attraverso l'abuso di identità digitale.
Ulteriori e gravi profili d'offesa di diritti anche fondamentali ed interessi meritevoli di protezione (penale) nel *Cyberspace* sono ravvisabili in tali fenomeni, a partire dalle conseguenze anche psicologiche sofferte dalle vittime[39], fino all'eventuale pregiudizio all'onore ed alla reputazione subìto dalla persona offesa[40], in ogni caso potendo essere coinvolte lesioni alla sfera più intima della riservatezza e dell'autodeterminazione informativa[41], accanto a profili di sicurezza e di certezza nel traffico giuridico informatizzato, di interesse di tutta la collettività nell'attuale dimensione globale della Rete.

---

[35] CIPOLLA, *Social network*, cit., 2675.

[36] Ibidem.

[37] FLICK C., *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, in *Dir. Inf.*, fasc. 4-5, 2008, 530.

[38] Una parte della dottrina ha cercato di ampliare la portata della fattispecie in esame, tentando di includere nella definizione di "danno" anche il "lucro cessante". Cfr. i riferimenti, su questo punto, di MALGIERI, *Il furto di identità digitale*, cit., 48 ss.; CRESCIOLI, *La tutela penale*, cit. In giurisprudenza cfr. Cass. pen., sez. II, 11 settembre 2013, n. 37170; Cass. pen., sez. II, 16 settembre 2009, n. 40790.

[39] Si pensi all'abuso di identità digitale che comporti il caricamento, su canali personali di social media o social network, di video a sfondo sessuale che vedono come protagonista la persona offesa.

[40] Si pensi alle ipotesi di abuso di identità digitale con cui vengono caricati, ad es. sul profilo personale di Facebook, frasi offensive, ovvero post con contenuti razzisti o aventi ad oggetto diverse forme di apologia.

[41] Si fa riferimento ai casi in cui l'abuso dell'identità digitale comporta l'accesso a spazi informatici riservati, contenenti dati personali, se non intimi o segreti.

5. Osservazioni conclusive: verso un mutamento di nozioni basilari quale quella di consumazione del reato nel *Cyberspace*?

Le questioni aperte dall'esame dei reati e delle attività illecite che si commettono nel *Cyberspace* sollecitano, in una prospettiva teorica più ampia, riflessioni generali di teoria del reato, che attengono alla stessa definizione di nozioni basilari come quelle di "azione" e di "evento", nonché dell'eventuale nesso causale, penalmente rilevanti nel *Cyberspace*, da rileggere alla luce delle trasformazioni che hanno determinato l'*automazione*, la *dematerializzazione*, l'*interazione* e l'*interdipendenza* delle attività e dei servizi che vi si svolgono.

In particolare, il concetto basilare di "fatto" tipico, costitutivo di reato, la cui commissione fonda l'applicazione della sanzione penale ed, a monte, l'attivazione delle indagini e degli eventuali strumenti cautelari, non può prescindere da quelle "porzioni" sempre più rilevanti che si realizzano *tramite* i sistemi informatici ed in rete, in esecuzione di programmi basati su algoritmi sofisticati e complessi, concepiti ed attivati da soggetti che ne sono comunque titolari o fruitori: fenomeni rispetto a cui occorre verificare in che misura siano anche giuridicamente imputabili alla "consapevole volontà" dell'uomo che li attiva o se ne serve. L'*autonomia* (seppur relativa) delle determinazioni e "scelte" operative dei sistemi informatici non sembra poterne escludere in linea di principio l'attribuzione (anche) alla sottostante "volontà" dei soggetti umani, da cui i sistemi stessi ed i loro *output* in ultima analisi necessariamente dipendono. Ma sono certamente da precisare i presupposti ed i limiti, in relazione ai quali può dirsi esercitato e mantenuto, ai fini della responsabilità penale, il "dominio" dell'uomo su tutti i risultati ed effetti che conseguono e permangono, spesso a grande distanza di tempo e di luogo.

Sulla base della definizione convenzionale di "sistema informatico" (cfr. *supra* § 2), e come si è visto anche nella soprastante analisi dei reati informatici in senso stretto ed, in particolare, nei casi paradigmatici dei delitti di frode informatica ed accesso abusivo (cfr. *supra* § 3.1), l'attività realizzata dal o se si vuole "tramite" il sistema stesso ha - già - una propria *specifica* rilevanza giuridica, tanto da essere espressamente sussunta nelle predette (come in altre) fattispecie penali sopra menzionate, con tutte le problematiche insorte per determinare anche il luogo ed il momento della consumazione.

Le evidenziate caratteristiche tecniche dell'*automazione*, che investe – oltre all'elaborazione - anche la circolazione, messa a disposizione, permanenza dei dati e dei contenuti nel *Cyberspace*, impongono dunque *in primis* di riconsiderare le condizioni alla cui stregua stabilire e circoscrivere il momento della "consumazione" del reato, *ivi* in tutto o in parte commesso.

Non solo, infatti, si espandono nel tempo e nello spazio i suoi "effetti" - come paradigmaticamente è emerso nel caso Google concernente il diritto all'oblio, affermato dalla sentenza della CGUE del 2014 proprio per stabilire un argine a tali fenomeni, evitando la violazione o limitando la compressione di diritti fondamentali della persona: è lo stesso "fatto" tipico che, nella parte in cui si realizza *tramite* i sistemi informatici, si deve ritenere che si protragga, espanda ed eventualmente "riproduca" in quei suoi elementi essenziali, che dipendono dall'esecuzione delle funzioni automatizzate di memorizzazione, trasmissione, messa a disposizione, condivisione, circolazione, ricerca, ecc., pur non sempre né del tutto "dominabili" dai titolari, gestori e fruitori dei sistemi stessi.

In altri termini: se non è corretto, nel contesto tecnologico descritto, attribuire indiscriminatamente la responsabilità penale per qualsivoglia anche più lontano – nel tempo e nello spazio – "effetto" di un qualsiasi intervento di un soggetto nel *Cyberspace*, non si può però neppure escludere *a priori* la rilevanza giuridica e penale dei predetti effetti quando siano elementi *costituivi* di reati cibernetici, né ridurne quindi la speciale durata ed espansione, nel tempo e nello spazio, ad un mero *post factum* non punibile, perché il prolungamento *automatizzato* dell'azione e/o dell'evento *tipici* non è affatto separabile dagli altri elementi oggettivi e soggettivi costitutivi del "fatto" di reato, di cui siano parte essenziale, essendo questo che viene piuttosto ad assumere connotati specifici, in ragione delle TIC

tramite cui l'autore lo ha (consapevolmente) posto in essere, con ogni conseguenza anche per gli eventuali partecipi e concorrenti in genere.

Al riguardo sembra utile muovere dall'applicazione ed eventuale adattamento alla realtà cibernetica della tradizionale distinzione dogmatica fra momento di "perfezione formale" del reato, che si ha quando ne sono realizzati tutti gli elementi costitutivi essenziali, seppur nel loro contenuto minimo, e momento di "esaurimento" o "consumazione sostanziale", che si ha solo quando esso ha per l'appunto "esaurito" *definitivamente* il proprio specifico contenuto di offesa, avendo raggiunto il massimo grado di lesione del ben giuridico protetto[42].

Ebbene, il reato cibernetico non può dirsi di norma "esaurito" nel periodo intermedio anche assai lungo che può intercorrere fra i due momenti, in cui "permane" e si approfondisce l'offesa. Tuttavia il fenomeno non pare neppure riconducibile al paradigma del reato permanente in senso proprio (come è ad es. il sequestro di persona), che presuppone, alla stregua della fattispecie legale, la costante dipendenza della protrazione dell'offesa al bene giuridico (nell'esempio: la libertà personale della vittima) dalla diretta e contemporanea *condotta volontaria* del reo, il quale potrebbe in ogni momento farla cessare (tanto che si parla addirittura, da taluni, di un reato misto di commissione per la realizzazione iniziale e di omissione per il successivo mantenimento dello stato antigiuridico)[43]. Essendo l'automazione specifica delle TIC che determina la diffusione nel *Cyberspace* e la protrazione nel tempo dei suoi effetti ancora potenzialmente attivi, questi possono sfuggire al diretto controllo dell'azione o comunque "dominio" da parte del reo, che pur lo ha posto inizialmente in essere loro tramite.

Neppure si attaglia perfettamente alle caratteristiche del reato cibernetico la nozione di reato "a consumazione prolungata", più recentemente sviluppata in giurisprudenza[44], in relazione a fattispecie, quali la corruzione o l'usura, che possono presentare momenti alternativi di consumazione, in quanto gli atti che le realizzano possono essere più d'uno, estendendosi ad abbracciare anche il od i pagamenti che seguono la promessa e l'accordo raggiunto fra le parti, che già formalmente perfezionano il reato, pur non esaurendone il contenuto offensivo, che si aggrava con i successivi versamenti. Infatti, tali atti successivi sono tutti direttamente dipendenti da più azioni volontarie di accettazione da parte dell'autore dei pagamenti ulteriormente posti in essere dal soggetto passivo.

Si prospetta, quindi, l'esigenza di delineare una categoria dogmatica nuova, che abbracci la peculiare, sempre più diffusa e rilevante realtà che si manifesta nella molteplicità di reati cibernetici configurabili nel *Cyberspace*, a partire da quelli di comunicazione e diffusione di un pensiero, nei quali non rileva un evento consumativo autonomamente verificabile nel mondo materiale, esterno cioè alla c.d. "infosfera" (quale ad es. può essere invece l'offesa al patrimonio altrui consumativa della frode informatica o dell'estorsione *on line*, che possono dirsi commesse nel tempo e luogo in cui si produce il danno altrui o si consegue l'ingiusto profitto, con tutte le problematiche che i moderni mezzi di pagamento *on line* comunque sotto altri aspetti sollevano[45]). La diffamazione *on line*, la diffusione di pedopornografia, l'istigazione e propaganda di atti di odio e discriminazione razziale, la distribuzione o messa a disposizione di opere digitali in violazione dei diritti d'autore, le molteplici violazioni della riservatezza e della *privacy*, compresi gli accessi abusivi, e molti altri reati cibernetici si consumano interamente ed esclusivamente nel *Cyberspace*.

---

[42] Su tale distinzione, pacifica nella teoria generale del reato, quantomeno da CARRARA, *Momento consumativo del furto* (1870), in *Lineamenti di pratica legislativa penale*, Torino, 1874, 229 s., e recepita da tutta la manualistica, non solo italiana, ma anche straniera (cfr. per tutti JESCHECK, WEIGEND, *Lehrbuch des Strafrechts. Allgemeiner Teil*, 5. Aufl., Dunker & Humblot, Berlino, 1996, 517 s.), cfr. volendo anche PICOTTI, *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali*, Milano, 1993, 568 s.

[43] Sulle conseguenze della durata nel tempo caratteristiche del reato permanente ed altri reati di durata, cfr. per tutti ROMANO M., *Commentario sistematico del codice penale*, I, 3^ ed., Milano, 2004, Pre-Art. 39, § 118 s., 344 s.; sul *postfactum* basti il rinvio alla monografia di PROSDOCIMI, *Profili penali del postfatto*, Milano, 1982.

[44] Per un quadro v. BRUNELLI, *Il reato portato a conseguenze ulteriori. Problemi di qualificazione giuridica*, Torino, 2000.

[45] Cfr. Cass., sez. VI, 4.10.1999 (dep. 14.12.1999), n. 3065; Cass. Sez. II, 11.11.2009 (dep. 20.11.2009), n. 44720.

Il "fatto di reato" dunque presenta in questi casi una "consumazione protratta" che si estende oltre il momento della perfezione formale, fino a che non giunga al momento (difficile, ma non impossibile da verificare) dell'esaurimento sostanziale, dovuto ad intervento dell'uomo od a ragioni tecniche. In questo anche molto prolungato periodo di tempo, e nella corrispondente estensione nello spazio, non pare dogmaticamente corretto ravvisare ancora gli elementi della *condotta* tipica, che deve sempre ricondursi al domino *attuale* della "volontà consapevole" dell'uomo, strettamente intesa.

Tuttavia è indubbio che l'offesa tipica, che ne è l'effetto, si produce in *conseguenza diretta* di siffatta condotta, volutamente e consapevolmente realizzata nel *Cyberspace*.

Sembra quindi delinearsi piuttosto una peculiare accezione di "evento", che pur se strutturalmente diversa dalla tradizionale nozione naturalistica, ne mantiene molte caratteristiche equivalenti, sul piano degli effetti sulla vittima e dell'offesa agli interessi protetti: per cui sembra poter essere imputabile non solo "causalmente", ma anche "soggettivamente" all'autore, a titolo di dolo (quantomeno eventuale), oppure di colpa, se ne ricorrano gli estremi, rispettando naturalmente i limiti personalistici propri della responsabilità penale.

La scelta del mezzo tecnico utilizzato (TIC), che implica l'automazione del trattamento e della circolazione in rete, con tutte le caratteristiche e conseguenze sopra richiamate, comporta che queste siano conosciute o quantomeno conoscibili dall'autore, che sceglie e *vuole* "agire" per l'appunto tramite le TIC.

Ne consegue che il momento consumativo, alla cui stregua determinare la legge penale applicabile (*ex* art. 2 c.p.), dovrà includere la fase ulteriore di "prolungamento" ed estensione dell'*evento* "cibernetico" (l'*output* nel *Cyberspace*), fermo il divieto di retroattività della legge incriminatrice o sfavorevole, rispetto al momento invece della condotta, in relazione alla quale soltanto può operare il contenuto precettivo della norma[46]; mentre la decorrenza del termine di prescrizione dovrebbe essere posticipato tendenzialmente fino al momento dell'esaurimento o consumazione sostanziale, dato il protrarsi dell'interesse punitivo fino a detto momento, come del resto previsto per i reati permanenti ed a consumazione prolungata (art. 158, comma 1, c.p., nonché art. 644-*ter* c.p. per quanto concerne l'usura).

Il *luogo* di commissione del reato, che deve coincidere con il luogo della consumazione, sembra invece da riferire a quello della perfezione formale e, dunque, della *prima* manifestazione dell'evento, come del resto conferma la regola prevista per i reati di omicidio e permanenti (art. 8, commi 1, 2 e 3 c.p.p.), salvo che l'evento "cibernetico" assuma immediati caratteri di "ubiquità" e perciò, non essendo possibile determinarlo, sia necessariamente quello "dell'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione" (art. 9, comma 1, c.p.p.), con risultati in concreto non diversi da quelli collegati al menzionato criterio dell'"inizio della consumazione" previsto per il reato permanente (art. 8, comma 3, c.p.p.).

Ne consegue, in ogni caso, che dovrà riconoscersi, in conformità ai principi generali, la configurabilità della partecipazione concorsuale penalmente rilevante *ex* art. 110 c.p., in forma sia attiva sia omissiva, da parte di terzi - compresi gli ISP, in relazione al ruolo attivo o di contributo alla circolazione e condivisione di contenuti in rete concretamente svolto - fino all'avvenuto "esaurimento", sulla base dei relativi presupposti oggettivi e soggettivi[47].

Evidenti sono le ricadute pratiche di tali conclusioni, nell'attribuzione di responsabilità penale agli operatori ed agli utenti della Rete, ad es. in un *social network* in cui si mantengano, inoltrino, approvino, facciano ulteriormente circolare *post*, messaggi, immagini penalmente lesive di diritti altrui, pur inizialmente trasmessi e prodotti da altri, che abbiano già "formalmente" *consumato*, ma

[46] Sul necessario riferimento al momento della condotta cfr. Cass., Sez.Un., 19.7.2018 (dep. 24.9.2018), n. 40986, Pres. Carcano, Est. Caputo, in www.penalecontemporaneo.it, con nota di ZIRULIA, *Le Sezioni unite* sul tempus commissi delicti *nei reati c.d. ad evento differito (con un* obiter dictum *sui reati permanenti e abituali)*.

[47] In tal senso si veda la sentenza della Corte di Cassazione 27.12.2016, n. 54946, nel c.d. caso Tavecchio, che ha confermato la condanna penale per concorso in diffamazione di un *blogger*, che aveva "mantenuto" il testo con le espressioni offensive sul proprio sito, nonostante fosse stato reso edotto del loro contenuto.

non ancora "sostanzialmente" *esaurito* il reato commesso, per il protrarsi e diffondersi dell'evento (od *output*) nel *Cyberspace*.

I limiti di garanzia da riaffermare sono certamente rappresentati dal principio di stretta legalità, con l'inerente divieto di estensione analogica delle fattispecie penali, e dal principio di colpevolezza, che impone di circoscrivere comunque la responsabilità penale ai "fatti" *personalmente* imputabili: e dunque, rispetto all'evento (od *output*) "cibernetico", nei limiti di spazio e di tempo, in cui esso sia riconducibile alla previsione e volontà dell'agente, da valutare al momento dell'azione, nel caso di reato doloso, ovvero alla sua prevedibilità ed evitabilità, riferibile anche al tempo in cui se ne protraggano le conseguenze, nel caso di reato colposo.

Un ampio campo ancora da esplorare, che investe questa ed altre nozioni basilari di teoria del reato – oltre a quelle di azione ed evento, si pensi anche quelle di causalità, di partecipazione criminosa, di tentativo, ecc.[48] - è dunque aperto alla riflessione ed elaborazione dogmatica del penalista, che per non venire meno al proprio compito di giurista, deve saper adeguare i propri strumenti conoscitivi e le proprie categorie concettuali alla nuova realtà, pur senza mai abbandonare i principi fondamentali e le garanzie invalicabili del diritto penale, propri di un ordinamento democratico.

[48] Cfr. volendo già PICOTTI, *Internet e responsabilità penali*, in PASCUZZI G. (a cura di), *Diritto ed informatica*, Milano 2002, 117 s.