Diritto @ Storia
Rivista internazionale di Scienze Giuridiche e Tradizione Romana
[ISSN 1825-0300]
N. 9 – 2010 – Contributi

IL CITTADINO NELLA "RETE" INFORMATICA: TUTELA PENALE E LIMITI DEL SISTEMA*

ADRIANA COSSEDDU
Università di Sassari

1. – Note introduttive

L'iniziativa pone all'attenzione una tematica non solo attualissima ma fonte di molteplici riflessioni, sia per l'orizzonte complesso in cui si innesta, sia per le sue implicazioni.

Anzitutto, due parole sul titolo: vorrei, per darne conto, prendere lo spunto da un recente Convegno intorno a una domanda: *Il diritto governa la tecnica?*[1] Assistiamo a una tecnologia che – si osserva – sottrae al diritto il territorio, ovvero il luogo nel quale ordinariamente si collocano le situazioni di vita e vengono tutelati rapporti giuridici e diritti. La "rete" globale muta le categorie, laddove tradizionalmente, specie in ambito penale, il fatto materiale viene realizzato nel «*mondo 'esterno' delle relazioni intersoggettive*»[2]. Lo spazio virtuale prende il posto della realtà fisica e l'intermediazione del sistema informatico o telematico diventa "strumento" capace di "ridisegnare" le stesse categorie della condotta e dell'evento, note al penalista.

Il contesto tecnologico evoca dunque un più ampio dibattito.

È il «dialogo» su diritto e tecnica, nel quale E. Severino, da filosofo, sottolinea una tecnica che «tende all'onnipotenza», ed il giurista N. Irti paventa nel discorso su quest'ultima la fine del diritto. Così, dinanzi ad una tecnica, a cui nulla può essere opposto e che esprime da sé le proprie regole, il giurista pone una domanda: «Perché il diritto tace? C'è un indebolimento del diritto nel nostro tempo?» O è incapace di «dominare le volontà?»[3].

Risponderemmo forse che la "ricca" produzione di norme, anche nel settore in oggetto, parrebbe oggi costituire per sé la più evidente smentita del dubbio posto; eppure, anche a non voler condividere la recente prospettiva di un "diritto senza scopo", quasi equiparabile a '*nomodotto*', un indebolimento, è vero, emerge per una ragione profonda, per quanto non la sola: il diritto e la sua storia si collocano nella territorialità, dove i confini si separano e si distinguono; il *computer* "opera" invece in tutti i luoghi e in nessun luogo[4].

Cruciale la domanda: come può un diritto indebolito inseguire un'assenza di spazio per la *s-confinatezza* insita nella globalità? Chi ne detta per essa le regole?

Proverei a tradurre la domanda per collocarla nel sistema penale: dinanzi ad una "rete" informatica che annulla la dimensione "spazio-temporale", dove si dialoga tra persone "senza volto", identità virtuali, e al contempo al di là di ogni barriera, quali risposte può offrire un diritto penale posto a confronto con una criminalità informatica dalle dimensioni trasnazionali? Quali nel *cyberspace* le note categorie che delimitano per il penalista il *tempus* e il *locus commissi delicti*[5]?

Già in epoca precedente agli interventi normativi in materia, si sottolineava la "genericità" dell'etichetta *computer-crimes*, posto che al dato linguistico non si conforma una corrispondente serie di fattispecie capaci di reprimere efficacemente tale forma di criminalità, allora nuova, ma oggi sfociata nelle molteplici modalità innovative di *cyber crime*.

Le ragioni: anzitutto, l'impressionante velocità di sviluppo e affinamento delle tecniche informatiche, che trovano in parallelo un altrettanto rapido 'adeguamento' nelle più varie forme di criminalità, che ne adottano un corrispondente uso illecito; di contro, un legislatore che si pronuncia in un tempo che può rischiare, per l'evoluzione della tecnologia, di essere già «obsoleto» nel momento stesso in cui traduce il suo intervento in norme di diritto positivo[6].

Un interrogativo ulteriore emerge nella dottrina penalistica a fronte di fattispecie già esistenti, ma per tanti di dubbia validità nel settore, collocate all'interno del codice penale a dettarne la disciplina: sono realmente configurabili vuoti di tutela nell'ordinamento, tanto da richiedere nuove incriminazioni, quasi in una sorta di «competizione» tra evoluzione della tecnica e legislazione[7]?

Proviamo dunque a descrivere le tappe essenziali del percorso normativo.

2. – Fonti normative e adeguamento del sistema

È ancora una volta il livello sovranazionale che fa emergere l'opportunità di specifiche incriminazioni per forme di criminalità informatica di maggiore rilevanza: il Comitato dei Ministri del Consiglio d'Europa adotta inizialmente la Raccomandazione N. R (89) 9, «sulla criminalità connessa agli elaboratori elettronici», indicando, in un «sommario dei principi direttivi per le legislazioni nazionali», un *elenco minimo* dei reati da prevedere accanto

ad un *elenco facoltativo*[8].

Nel primo, fra gli altri, il reato di *frode informatica*, ovvero, la fattispecie di ingresso, alterazione, cancellazione o soppressione di dati o di programmi informatici o qualsiasi altra ingerenza in un trattamento informatico, che ne influenzi il risultato, causando un pregiudizio economico o materiale ad altra persona (ed ulteriori 'varianti'). Ancora: il *falso informatico*, descritto per analoghe tipologie di condotte, ma con modalità o condizioni capaci di riprodurre, in conformità al diritto nazionale, ipotesi di falso; altra previsione, l'*accesso non autorizzato* ad un sistema o ad una rete informatica, ovvero, in assenza del relativo diritto e in violazione delle regole di sicurezza.

La nuova prospettiva ha da subito posto un primo livello di confronto, emerso in dottrina nell'indefettibile riferimento ai contenuti propri della nostra Carta costituzionale, dove l'informatica non entra a disegnare un suo spazio di tutela neanche implicita; eppure, si ritiene che beni più tradizionali, quali fede pubblica, patrimonio, economia pubblica, non siano capaci di esaurire il disvalore insito nella maggior parte dei c.d. crimini informatici. Da qui la prospettata necessità di un denominatore comune espresso nella formula «intangibilità informatica» quale "nuovo" bene giuridico in materia[9].

Segue, nel nostro ordinamento, la L. 23/12/1993 n. 547, *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, quale risposta ad una necessaria «esigenza di non costringere ancora una volta la giurisprudenza ad un intervento di supplenza»[10], funzione del resto confliggente con il fondamentale principio di legalità, nel suo corollario della tassatività, principio di portata costituzionale vigente in materia penale.

La scelta del legislatore nazionale nel settore si è peraltro collocata in un crinale tra nuove incriminazioni, accomunabili in base al loro strutturale collegamento con i sistemi elettronici e informatici[11], e antiche collocazioni codicistiche.

In rapporto all'operatività dei sistemi informatici o telematici, se n'è tracciata una mappa secondo le tipologie:

- **reati *a mezzo* dei sistemi informatici o telematici**, ovvero realizzabili con l'utilizzo dei predetti sistemi, quale la *frode informatica*, art. 640 *ter* c.p.
- **reati *contro* sistemi informatici o telematici**, caratterizzati per l'oggetto materiale riferibile ai predetti sistemi.

Tra le fattispecie, in ragione dei profili in questa sede di un qualche rilievo:

a) *il danneggiamento di sistemi informatici o telematici* (ipotesi, per tipologie differenti, riconducibile agli artt. 635 *bis* ss., ma anche all'art. 615 *quinquies* c.p.);

b) *l'accesso abusivo a sistemi informatici o telematici* (art. 615 *ter* c.p.);

c) *la detenzione e diffusione di codici di accesso* (art. 615 *quater* c.p.);

d) *ipotesi di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche* (artt. 617 *quater* e *quinquies* c.p.).

Da ultimo, le fattispecie di "falsificazione" ridefiniscono i propri confini: a vario titolo e con diverso oggetto sono ricostruibili, da un lato, a margine dell'art. 491 *bis* c.p., concernente il «documento informatico», dall'altro, si estendono in riferimento al contenuto delle «comunicazioni informatiche o telematiche», di cui al nuovo art. 617 *sexies* c.p. Collocato tra le norme a tutela della «inviolabilità dei segreti», quest'ultimo è seguito dalla norma di chiusura ed estensiva della tutela, che è oggi l'art. 623 *bis* c.p. (concernente «*Altre comunicazioni e conversazioni*»).

Un'altra tappa, in materia di criminalità informatica, è stata segnata dalla Convenzione del Consiglio d'Europa firmata a Budapest il 23 nov. 2001, ed ora ratificata in Italia con la L. 18 marzo 2008 n. 48 [12]. Alla riformulazione della definizione di *documento informatico*, *ex* art. 491 *bis* c.p., si sono aggiunte ulteriori modifiche, integrazioni ed innovazioni, all'interno fra l'altro del codice penale: nuove ipotesi, inserite tra i delitti contro il patrimonio, attengono al *danneggiamento* di informazioni, dati e programmi, e ad analoghe condotte su sistemi informatici o telematici (artt. 635 *ter*, *quater*, *quinquies* c.p.); vi si aggiunge la riformulazione dell'art. 615 *quinquies*, sulla *diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*, ipotesi quest'ultima diversamente collocata nell'ambito dei delitti contro l'inviolabilità del domicilio (e quindi, contro la persona).

Una breve notazione nel merito: la tecnologia propria del settore porta, con la evidente "de-localizzazione" del «fatto» posto in essere, un *anonimato* che tende come tale a 'mascherare' il volto reale dell'autore della condotta criminosa, per far coincidere con la solitudine lo "spazio" abitato dalla vittima, quest'ultima, con volto certo!

Si può in proposito rilevare come nuove esigenze di tutela si consolidino a livello normativo a favore del cittadino, riconoscibile comunque come tale anche in una sua identità virtuale; eppure, complessa ne è la trama rispetto ad una ricostruzione all'interno del sistema vigente.

Verifichiamo, pur sommariamente, le risposte dell'ordinamento.

A fronte della previsione oggetto del Titolo I della Convenzione di Budapest del 2001 - concernente «*Offences against the confidentiality, integrity and availability of computer data and systems*» - si deve operare un'indagine nella dottrina per rinvenire e far emergere nel nostro sistema normativo, quale categoria giuridica, la "riservatezza informatica o telematica", da assumere come bene oggetto di tutela.

Difatti, la collocazione codicistica delle fattispecie in questione è per sé varia: taluna fra le altre è inserita tra i *delitti contro l'inviolabilità del domicilio*; citiamo per tutte l'*accesso abusivo ad un sistema informatico o telematico* (art. 615 *ter* c.p.).

Nel merito si potrebbe obiettare come la categoria giuridica in parola, oggetto degli artt. 614 ss. c.p., investa come tale nella sua *inviolabilità* un ulteriore aspetto della libertà della persona, da intendersi quale "proiezione spaziale" della personalità del soggetto stesso. Il medesimo concetto di *domicilio* è stato altrimenti esteso ed enucleato in un concetto di «domicilio informatico»[13], ovvero, "spazio ideale di pertinenza della persona", cui

estendere la tutela della riservatezza della sfera individuale, bene costituzionalmente protetto e qualificabile in forza della più estesa titolarità da parte del soggetto di uno *ius excludendi alios*, anche rispetto ad un sistema informatico.

Eppure non manca chi fa rilevare la singolarità della collocazione sistematica di fattispecie, come quella in parola, verosimilmente orientata ad una *riservatezza* non tanto domiciliare, quanto piuttosto rivolta a taluni aspetti esteriorizzati della personalità[14]. Del resto, si può con altri sottolineare come la collocazione materiale dei sistemi informatici e telematici sia in sé indifferente rispetto a un domicilio, ed anzi sia spesso extra-domiciliare[15]: si pensi all'utente *home banking* rispetto a spazi riservati nell'ambito dell'istituto di credito o a servizi in rete.

Analogamente, in merito alle altre fattispecie inserite nel codice penale nell'originaria categoria dei *delitti contro l'inviolabilità dei segreti*, si è voluto distinguere in dottrina tra i delitti propriamente inerenti alla *inviolabilità della corrispondenza*, e i delitti contro *l'inviolabilità delle comunicazioni*, oggetto in particolare delle fattispecie inizialmente introdotte con la L. 8 aprile 1974 n. 98 (*recante norme per la tutela della riservatezza e della libertà e segretezza delle comunicazioni*), e successivamente inserite in taluni moduli normativi, all'interno del codice, dalla citata legge del '93.

Nell'analisi a margine, si è inteso ulteriormente distinguere al loro interno tra delitti contro la *riservatezza delle comunicazioni*, e delitti contro *la libertà delle comunicazioni*, individuata quest'ultima nel «diritto di trasmettere ad un destinatario determinate forme espressive senza altrui impedimenti, interruzioni, falsificazioni»[16].

Un complesso quadro normativo si snoda dunque tra interessi inerenti alla sfera più propriamente privata, quale la *riservatezza*, ed altri riferibili piuttosto, per contenuto, alla *fede pubblica*, ravvisabile nell'affidamento del pubblico circa i mezzi usati in ragione di una rappresentazione e certezza delle relazioni giuridicamente rilevanti[17]. *Autenticità*, *genuinità* sono categorie che emergono anche nell'ambito al quale non può risultare certo estraneo il "traffico giuridico", che si avvalga di strumenti informatici e telematici.

Ma alle manipolazioni connesse alla diffusione dell'informatica corrispondono spesso le più diverse aggressioni non solo a un'identità "virtuale", ma anche al patrimonio altrui, quello sì reale, con vantaggi anche cospicui per l'autore o terzi; sono condotte poste in essere con modalità fraudolente, che stentano a trovare nell'ordinamento, tra l'eterogeneità delle fattispecie e l'incertezza dei significati ascrivibili alle espressioni normative[18], un "approdo sicuro" in termini di tutela.

Prima di accennare ad un'esemplificazione, altre fonti attestano la complessità della "rete", quale fenomeno dalle molteplici potenzialità, ma le cui connessioni diventano per il cittadino, al contempo, 'luogo di relazioni', dove la libertà è sperimentabile in incontri virtuali, e 'limite' alla stessa nell'esposizione a rischi, difficilmente controllabili – si fa notare – in sede penale, sistema tradizionalmente improntato al "*face to face*".

Una complessità dunque sul piano normativo, di cui è prova la Decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione e nel cui ambito la criminalità organizzata costituisce una minaccia sempre più avvertita, a fronte dell'obiettivo di «uno spazio di libertà, sicurezza e giustizia» in ambito UE.

Ne è prova la Comunicazione della Commissione delle Comunità Europee al Parlamento Europeo, al Consiglio e al Comitato delle Regioni (22.5.2007) «Verso una politica generale di lotta contro la cibercriminalità».

Vi si legge l'urgenza di intervenire a livello nazionale ed europeo contro tutte le forme di reato informatico, quale minaccia sempre più grave. «La protezione del singolo dalla cibercriminalità si scontra spesso con problemi connessi alla determinazione della giurisdizione competente, del diritto applicabile, all'attività di contrasto trasnazionale».

Tra i moltissimi reati si segnalano per essere «particolarmente comuni e in aumento […] le frodi [...] di vario tipo, mentre il furto d'identità, il *phishing* (ovvero, il tentativo di acquisizione fraudolenta di informazioni sensibili, come *password* o estremi di carte di credito, fingendosi una persona di fiducia in una comunicazione elettronica), lo *spam* e i codici maligni sono strumenti che permettono frodi su larga scala». Si sottolineano gli strumenti giuridici esistenti nella lotta alla criminalità, ma al contempo si sollecitano adeguamenti normativi, in particolare circa «i reati informatici connessi al **furto d'identità**», ovvero all'uso di dati di identificazione personale (come il numero di carta di credito) per commettere altri reati; fattispecie quest'ultima non prevista in tutti gli Stati membri, eppure – si fa rilevare – più facile da provare rispetto al reato di frode. L'evoluzione che, parallelamente alla tecnologia informatica, emerge nella tipologia delle attività criminose ha fatto registrare un numero di frodi bancarie aumentato, con il sistema c.d. *Phishing*, dell'*8000%* solo negli anni 2006/2007 [19].

Proprio in Italia il legislatore del '93, posto dinanzi alle scelte d'incriminazione dettate dalla Raccomandazione, di cui si è dato conto, non ha introdotto una fattispecie *ad hoc* per il c.d. "furto di dati"; né l'utilizzo senza diritto di identità virtuale, o la raccolta, o acquisizione di dati riservati facenti capo ad un soggetto si può configurare *in sé* quale forma di "impossessamento" mediante sottrazione di una *res* altrui - elementi, diversamente costitutivi del reato di furto, almeno quale tipizzato dall'art. 624 c.p. Il soggetto titolare, che *inconsapevolmente* rende noti i propri dati in risposta ad una richiesta ingannevole via *e-mail*, continua infatti a disporre dei medesimi senza che se ne possa assumere, in ipotesi, la corrispondente privazione, divenendo pertanto "vittima" non già di un'usurpazione unilaterale fondata sul proprio dissenso, ma in forza della sua stessa, "inconsapevole" collaborazione!

Sulla scia di ulteriori sollecitazioni si collocano le Conclusioni del Consiglio (2009/C 62/05, in Guue 17.3.2009) del 27 nov. 2008, *relative ad una strategia di lavoro concertata e a misure pratiche di lotta alla criminalità informatica*: a fronte delle «forme tradizionali di criminalità commesse via Internet, quali l'usurpazione di identità, il furto d'identità, le vendite fraudolente», ecc., si invitano gli Stati membri e la Commissione a predisporre misure di contrasto, e nel breve termine «la definizione del concetto di "usurpazione d'identità su Internet", conformemente alle legislazioni nazionali».

La complessità già evidenziata all'interno del sistema, dinanzi a una pluralità di norme di varia collocazione, suscita dunque quesiti ulteriori, se è vero che si invocano "nuove" previsioni per un efficace contrasto alla

criminalità informatica.

Non è evidentemente possibile all'interno del sistema penale, e in questa sede, una disamina delle fattispecie a vario titolo inserite nell'ordinamento, ma valga per tutte l'esemplificazione di modalità illecite ricorrenti, e sempre più diffuse e sofisticate, che peraltro non trovano risposte univoche, ancor prima che nelle aule di giustizia, attraverso una lettura "certa" delle numerose norme presenti nel sistema.

Muoviamo da un dato: non esiste una norma incriminatrice che espressamente 'riproduca' la condotta di *phishing*, non inquadrabile per la sua articolazione, di cui si dirà, nella fattispecie che nel *nomen iuris* parrebbe evocarne la rispondenza, ovvero, la *frode informatica*, *ex* art. 640 *ter* c.p.

Si è autorevolmente rilevato che tutte le nuove forme di "truffe informatiche" sono precedute dal c.d. "furto d'identità digitale", che «consente all'autore di agire "indisturbato"», all'interno di una "rete" che non fa trapelare la sua identificazione[20], ma che evidentemente si muta in una 'trappola' per la vittima.

Si evidenzia nella terminologia la mancata corrispondenza tra "nomenclature", correnti e ricorrenti, e concetti esplicativi di 'fenomeni' come tali non immediatamente traducibili per il diritto, almeno per un sistema penale che necessita di fattispecie determinate e precise a garanzia della fondamentale certezza del diritto e tutela del cittadino. Anche la fattispecie della frode informatica, *ex* art. 640 *ter* c.p., risulta, come accennato, inapplicabile se realizzata in assenza dell'alterazione del funzionamento di un sistema informatico o di intervento manipolativo sui dati, modalità che ne configura l'elemento costitutivo; lo stesso comportamento investe del resto non già la sfera inerente alla persona in quanto tale, bensì il sistema informatico di pertinenza, quale "spazio informatico" ad essa riservato.

3. – *Phishing*: analisi del fenomeno e indagine normativa

Per restare nella quotidianità che tutti ci interpella, mi limiterei a qualche cenno a quella che viene definita "metodologia dell'attacco" del più volte citato *phishing*, per verificarne l'inquadramento normativo nelle sue diverse fasi, quali usualmente descritte:

1) formazione dell'*e-mail* non veritiera, che imita gli estremi identificativi di un mittente reale – Banca, Posta, ecc. – e ne adotta il linguaggio nella comunicazione; conseguente invio del *messaggio* ad uno o più soggetti: è il c.d. meccanismo di *social engineering*, con il quale vengono carpite informazioni riservate, *userid*, *password*, di utenti *home banking* da utilizzare successivamente dal *phisher* per operazioni in frode e a danno dell'utente correntista.

Emerge, già *prima facie*, l'assenza di una norma per sé corrispondente alla condotta descritta, mentre la risposta normativa conseguente si diversifica nell'interpretazione; cercheremo di darne brevemente conto.

Si ipotizza, a margine della condotta, l'integrazione della fattispecie di sostituzione di persona, *ex* art. 494 c.p., delitto contro la fede pubblica, configurabile nel momento in cui vengono utilizzati gli estremi identificativi *on line* di un mittente reale. Gli elementi della fattispecie devono tuttavia riflettersi nel fatto. Ed è a fronte degli stessi che la *sostituzione* illegittima della propria all'altrui persona, quale normativamente prevista, parrebbe piuttosto indicare l'ipotesi di una persona fisica *individuabile* nella sua qualità di mittente, elemento diversamente dubbio nel caso in esame, per le modalità impersonali del ricorso ad estremi identificativi di un "organismo", o istituzione, secondo tipologie virtuali (si imitano *look – feel* di loghi e sito). Parallelamente, rispetto alla Banca o all'Ente, al quale connettersi successivamente con l'utilizzo dei codici utente o dati identificativi 'carpiti' al destinatario dell'*e-mail* di *phishing*, difficilmente risulterebbe integrato l'ulteriore elemento normativo della fattispecie costitutivo dell'induzione in errore, in quanto i codici di accesso, a cui risponde l'elaboratore, sono *formalmente* corrispondenti all'identità virtuale del cliente[21].

Nell'una e nell'altra direzione non parrebbe immediatamente ravvisabile un'offesa alla pubblica fede, descritta dalla norma in ragione dell'identità, dello stato, delle qualità giuridicamente rilevanti della persona. La giurisprudenza di legittimità (Cass. Pen., Sez. V, 8 nov. 2007, n. 46674) ne ha assunto di recente la configurabilità tramite la rete *internet*, ma a fronte della creazione di un *account* di posta elettronica, con assunzione da parte dell'autore di falsa identità, comunque riferibile a persona determinata.

La fattispecie, *in sé* discussa anche in sede di promulgazione del codice penale sul presupposto di una fiducia accordata «*intuitu personae*» e ritenuta come tale 'estranea' alla categoria della pubblica fede, ha trovato anche di recente un'interpretazione che ne sottolinea tale peculiarità. Nell'ambito della giurisprudenza di merito si è difatti puntualizzato che anche "spacciarsi" per dipendente di un ente pubblico o privato «non integra una sostituzione ad altra persona, poiché tale sostituzione implica la indicazione specifica della persona sostituita». La punibilità atterrebbe dunque solamente all'agente il quale assuma «falsamente connotati che ineriscono strettamente alla persona e finiscono per individuarla specificamente». La dichiarazione risulterebbe certo falsa, ma non essendo indicata la persona sostituita, nemmeno sussisterebbe l'attribuzione di un *falso nome*. Analogamente, sarebbe da escludersi l'attribuzione di un *falso stato*, da intendersi quest'ultimo quale posizione rivestita dal soggetto nella società civile o politica; nemmeno dalla *falsa autoattribuzione della qualità* di dipendente potrebbero discendere effetti giuridici particolari – come dalla norma richiesto –, e certo «non il dovere (...) – si rileva – di fornire alcun dato personale a chi si qualifichi in quel modo»[22].

Se, dunque, nell'ipotesi in cui la persona sostituita rimanga «assolutamente indeterminata» si prospetta l'esclusione della fattispecie *ex* art. 494 c.p., così come la si esclude a fronte di una «falsa autoattribuzione di ogni e qualsiasi qualificazione individuale», non suscettibile come tale di spiegare effetti giuridici verso la persona offesa, ancora più incerti risulterebbero – di contro alla *forma vincolata* che tipizza la fattispecie – i confini normativi nel nostro caso. Di più. Nella sentenza di merito, qui richiamata, si ipotizza l'eventualità di altro delitto, come la truffa, di cui peraltro risulterebbero carenti, nel caso di specie, gli ulteriori elementi costitutivi.

Non sarebbe al contempo trascurabile, a margine dei dati forniti dall'ABI nel corso dell'Audizione alla Commissione finanze della Camera dei Deputati il 10 nov. 2009, quanto emerso nella relazione illustrativa del disegno di legge assegnato in sede referente, il 9 dicembre 2009, alla 2a Commissione permanente (Giustizia). Si tratterebbe delle «modifiche al codice penale e al codice di procedura penale per favorire il contrasto al furto

d'identità», provvedimento con il quale si propone di introdurre – quale norma '*ad hoc*' – l'art. 494-*bis*, onde sanzionare la «*frode con falsa identità*», ovvero l'indebita acquisizione «in qualsiasi forma» di «dati identificativi personali, codici di accesso o credenziali riservate». La punibilità si estende, nella previsione proposta, a chiunque «in qualsiasi modo formi, ricostruisca o diffonda informazioni individuali relative a persone fisiche o giuridiche al fine di organizzare attività fraudolente mediante assunzione abusiva dell'identità altrui (...), anche attraverso l'invio massivo di corrispondenza informatica ingannevole (...)».

Valga nel merito un rilievo ulteriore: il disposto dell'art. 494 c.p. nella formulazione vigente è norma sussidiaria, e come tale cede dinanzi al configurarsi di un altro delitto contro la fede pubblica. Si ipotizza nel merito un'interpretazione alternativa: l'eventuale applicabilità dell'art. 491 *bis* c.p. sul falso riferibile al «documento informatico», nel combinato disposto con l'art. 485 c.p., che sanziona la falsità in scrittura privata. Ne viene peraltro rilevata l'esclusione, soluzione parsa preferibile soprattutto in considerazione della tipologia propria dell'*e-mail*. Si tratta infatti in ipotesi di una comunicazione informatica sprovvista dell'efficacia probatoria, quale richiesta ad integrare la fattispecie di "falsità" nella ulteriore estensione alla *species* documento informatico[23].

Quale tutela dunque per il cittadino?

Forse, quella che si prospetta come tesi minoritaria, ed a margine di una norma ritenuta poco o nulla significativa nelle sue implicazioni pratiche, potrebbe offrire una qualche soluzione applicativa, peraltro adottata anche in una recente pronuncia di merito: tra le diverse innovazioni, l'art. 617 *sexies* c.p., *Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*, dispone: «Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni». Sulla base di una identità di modulo descrittivo con il precedente art. 617 *ter*, rispetto al quale si sostituisce l'espressione «comunicazioni telegrafiche o telefoniche» con l'altra, «comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi», si sottolinea che le modalità della condotta danno vita ad un *quid* riferibile al c.d. autore apparente, diverso dal reale[24]. Analogamente, l'espressione *formare falsamente* manterrebbe il significato di «creare *ex novo* il documento facendone risalire la paternità del suo contenuto ad un soggetto diverso dall'agente». Non diverso parrebbe l'inganno ai danni dell'utente, che interviene nell'ambito di eventuali 'rapporti di fiducia' da quest'ultimo instaurati con enti o istituti, e rispetto ai quali l'agente si interpone spendendo, presso il destinatario, la *falsa* provenienza del "messaggio" contraffatto. Se dovessimo adottare nella definizione del c.d. *phishing* l'espressione, riportata a margine della Comunicazione della Commissione dianzi citata (Bruxelles, 22.5.2007) ovvero, «tentativo di acquisizione fraudolenta di informazioni sensibili, […], fingendosi una persona di fiducia in una comunicazione elettronica», parrebbe la condotta fin qui descritta, a margine dell'art. 617 *sexies* c.p., non esserne lontana.

Intesa del resto, di recente, la «comunicazione» in oggetto sotto il duplice profilo statico e dinamico[25], formarne falsamente il contenuto significa – secondo quanto detto – crearlo *ex novo*, il che escluderebbe il "ruolo condizionante" dell'intercettazione, per sé riferibile piuttosto alle alternative ipotesi di alterazione e soppressione. La collocazione codicistica ne sottolineerebbe altresì in termini di tutela l'interesse protetto, individuabile nell'autenticità e genuinità della comunicazione nel suo riferirsi alla sfera personale. L'ulteriore utilizzo della falsa comunicazione, che la norma ai fini della perfezione del reato richiede, diventa elemento costitutivo interno alla fattispecie, di cui è ammissibile la forma tentata.

2) Ma, ad introdurre la seconda fase, altri dati emergono: il contenuto del messaggio di posta elettronica recante false richieste o notazioni e il *link* che indirizza ad una pagina *web* non autentica corrisponderebbero al contempo agli *artifizi e raggiri* previsti dalla fattispecie di truffa, *ex* art. 640 c.p., cui segue evidentemente l'induzione in errore dell'utente, spinto dalla falsa rappresentazione del reale a rivelare i dati fittiziamente richiesti.

Può dunque ritenersi configurabile la truffa nei suoi elementi? Laddove nella lettura del 'fenomeno' l'indirizzo emergente nella giurisprudenza farebbe propendere per una risposta positiva ravvisando un concorso di reati, riterremmo diversamente in ipotesi mancante quel requisito, noto come requisito "tacito" della truffa, che è l'atto di disposizione patrimoniale, in cui consiste la collaborazione della vittima. La consapevolezza di quest'ultima e l'atto cui consegue la diminuzione del patrimonio devono tradurre il convincimento erroneo del soggetto passivo in «un atto consapevole nella propria sfera patrimoniale», causa per la vittima del danno e per l'autore del profitto[26].

Nel caso di specie, salva l'ipotesi prospettata di un'esecuzione diretta del bonifico da parte dell'utente ingannato, è piuttosto il *phisher* stesso che, acquisiti i dati riservati, accede abusivamente al sistema bancario dell'utente, causando a quest'ultimo un danno patrimoniale anche di rilevante entità. Se così è, mancherebbero in ipotesi, pur presenti gli artifici e raggiri, gli ulteriori elementi integranti la fattispecie incriminatrice della truffa, che sopravviverebbe, per così dire, a denotare il disvalore della condotta, ma non a riprodurre la previsione normativa.

3) La fase che segue, a fronte della risposta adesiva dell'utente *on-line* indotto in errore, è l'acquisizione dei dati riservati dell'utente medesimo; credenziali con le quali il *phisher* opera successivamente l'accesso abusivo e le operazioni a suo profitto.

Le norme concorrenti a sanzionare le condotte nel loro susseguirsi sarebbero, rispettivamente, gli artt. 615 *quater* (il cui *nomen iuris* non è corrispondente al contenuto normativo), integrato fra l'altro dal procurarsi abusivamente «codici, parole chiave, o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza», in presenza del fine di procurare a sé o ad altri un profitto, o arrecare ad altri un danno; e 615 *ter*, che sanziona l'*accesso abusivo* ad un sistema informatico o telematico.

Alcune notazioni s'impongono nell'analisi strutturale: la prima delle due norme, art. 615 *quater* c.p., conterrebbe la previsione di una condotta, che nel "procurarsi" i dati riservati o «altri mezzi idonei all'accesso», risulta prodromica per le sue modalità rispetto all'accesso abusivo, di cui all'art. 615 *ter*, previsione peraltro precedente nella collocazione codicistica.

Quest'ultima, più grave nella sanzione, ma procedibile (in assenza delle ipotesi circostanziali previste) a querela della persona offesa, si riterrebbe la sola norma in ipotesi applicabile: infatti, al verificarsi dell'accesso

abusivo, l'art. 615 *quater*, integrato dalla condotta del procurarsi abusivamente le c.d. "chiavi d'accesso" al sistema, costituirebbe un antefatto non punibile rispetto al successivo utilizzo delle credenziali di accesso al sistema medesimo.

Un concorso apparente di norme, dunque, ma modulato su un'operatività condizionata nella scelta della norma prevalente, ovvero l'art. 615 *ter*, dalla procedibilità a querela; potremmo allora, in assenza di quest'ultima condizione di procedibilità, ritenere eventualmente applicabile, presenti gli elementi costitutivi, l'art. 615 *quater*, la cui meno grave previsione sanzionatoria (in riferimento alla pena detentiva) comporta di contro una procedibilità d'ufficio.

Il dato non è di poco conto, specie qualora, escludendo per via interpretativa l'applicabilità dell'art. 617 *sexies* a sanzionare il ricorso all'*e-mail* fraudolenta per "pescare" i dati riservati dell'utente, si ritenga la previsione del "procurarsi" abusivamente tali dati – *ex* art. 615 *quater* – inclusiva per sé dell'uso di *e-mail* finalizzata al prelievo dei dati stessi, in presenza evidentemente dell'elemento soggettivo richiesto. Un percorso complesso e letture pur sempre parziali.

Dunque, tante norme, o, come si è rilevato[27], «"spreco legislativo di fattispecie"» e pur tuttavia possibili "vuoti" di tutela?

Un'ulteriore disposizione può da ultimo soccorrere lo "sprovveduto" utente, qualora, ottenuti i dati riservati, l'autore della condotta illecita ne operi l'utilizzo indebito attraverso, ad es., operazioni di ricarica delle carte di credito pre-pagate (per un caso di specie, G.I.P. Trib. Milano, sent. 10 dic. 2007, n. 888: l'attività criminosa consisteva, fra l'altro, nel far confluire le somme di denaro presenti sui conti correnti e sulle carte pre-pagate delle vittime verso conti correnti appositamente attivati o altre carte pre-pagate acquisite dall'associazione criminale; rispettivamente, sistema da contocorrente a *postepay*, o da *postepay* a *postepay*).

L'ipotesi è sanzionata, attualmente, nell'ambito dell'art. 55, comma 9, D.Lgs. 21 nov. 2007 n. 231, in materia di misure antiriciclaggio, ed è riferibile a «chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi».

Si può in merito condividere l'opinione[28] – anche se riferibile ad analoga previgente previsione – per la quale il *danno*, pur non espressamente richiesto, sia insito nell'offesa contenuto del reato di utilizzo indebito, quale elemento del fatto (da non confondersi con il danno risarcibile); ne costituirebbe riprova l'interesse protetto, focalizzato nella sua valenza patrimoniale (cui da altri si aggiunge, anche in riferimento alle ulteriori ipotesi ivi previste, l'affidamento che discende dall'impiego di mezzi di pagamento alternativi al denaro contante).

Nella varietà delle previsioni richiamate un elemento, per così dire, "collettore", potrà ancora una volta rinvenirsi, ma è dato affidato al caso concreto, nella configurazione di un'eventuale "continuazione" nel reato, laddove un "medesimo disegno criminoso" ricorra, e parrebbe indubitabile, ad unificare *ex* art. 81, cpv., c.p., le diverse condotte illecite, integrative delle fasi dianzi descritte.

4. – Rilievi conclusivi

In conclusione, il sistema di tutela penale volto all'inviolabilità delle comunicazioni si misurerebbe oggi nel confronto con il più ampio contesto costituzionale degli artt. 15 («La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili»), 13 («La libertà personale è inviolabile») e 14 Cost. («Il domicilio è inviolabile»), dettati normativi volti ad assicurare «il *minimo* "inviolabile" di garanzia della libertà della persona umana, incentrato non solo sulla libertà fisico-psichica e sull'inviolabilità di una certa sfera spaziale, ma anche sull'inviolabilità delle comunicazioni interpersonali, costituenti una delle forme più dirette ed immediate di collegamento della persona con il mondo esterno»[29].

Dal "*right to be alone*", ovvero "diritto ad essere lasciato solo", l'obiettivo di tutela si sposta dunque, nella dimensione della "rete", sull'insieme della persona, di cui si chiede la protezione al di là di singoli aspetti, che ne costituiscono altrettante "forme" di espressione[30].

È la libertà personale che si relaziona con ogni altro, attraverso il "filtro" del mezzo informatico, capace peraltro di generare al contempo un'alterazione nel rapporto fiduciario per identità mascherate. Si comprende allora la ricorrente sollecitazione ad una previsione che tipizzi il c.d. "furto d'identità"; meglio diremmo, il fenomeno di *appropriazione* dei dati di un'altra persona, nel cui nome il soggetto effettui, con utilizzo indebito dell'altrui identità (anche fraudolentemente carpita), operazioni a suo vantaggio, in danno della vittima.

Ma forse, ed ancor prima, occorrerebbe ricercare una chiave di lettura univoca all'interno del sistema sulla base delle norme vigenti.

È comunque significativo che già nel Progetto del 1992 di riforma del Codice Penale[31] si collocasse, tra i reati inerenti alla persona, nella sua proiezione nei rapporti patrimoniali, una fattispecie da prevedersi tra i reati con la cooperazione del soggetto passivo: tale, all'art. 83 – 4) *l'abuso di mezzi informatici o automatici, consistente nel fatto di chi, avvalendosi in modo fraudolento o abusivo di tali mezzi, procura a sé o ad altri un ingiusto profitto con altrui danno. Prevedere la stessa pena per il fatto commesso con carte di credito o di pagamento ovvero con altri documenti analoghi che abilitino all'acquisizione di beni o servizi*.

Se oggi emerge, accanto o a superamento di una concezione piramidale dell'ordinamento, una concezione che evoca "l'immagine reticolare" del diritto, è altresì vero che la stessa, collocata in una dimensione informatica ed *a-spaziale*, che investe il diritto stesso, ben si rappresenta per immagini riferite a due componenti:

il **nodo**, a raffigurare «"tanto un legame che unisce, quanto qualcosa che lega"»;

la **rete**, che nella sua ambivalenza «può essere tanto la rete del tessuto, quanto la rete di una trappola...»[32].

Occorre forse, in vista della "protezione" tradizionalmente affidata al diritto penale per interessi ritenuti meritevoli di tutela, ripensare piuttosto, anche nella *comunicazione* - o soprattutto in essa - ad una "rete" di

relazioni, dove la persona, per la sua costitutiva dimensione relazionale, non resti avvinta quale possibile "preda"; è la garanzia da accordarsi al soggetto, affinché veda non solo tutelata, bensì pienamente *riconosciuta* nella "trama" dei rapporti la sua personalità.

Ma quest'ultimo, probabilmente, è orizzonte che esula dal diritto penale.

---

*Testo riveduto, e corredato dalle note essenziali, della Relazione svolta al Convegno organizzato a Sassari (5 febbraio 2010) dalla Banca d'Italia, di concerto con la Facoltà di Giurisprudenza dell'Università degli studi di Sassari e gli Ordini degli Avvocati, Notai e Dottori Commercialisti, dal titolo: *Dal contante alla moneta elettronica evoluzione del sistema dei pagamenti: opportunità, rischi e presidi di sicurezza*.

[1] L'espressione riproduce il titolo del Convegno che, in data 16 dicembre 2008, si è svolto a Roma presso il Cnel. L'incontro, avente ad oggetto una riflessione sul rapporto diritto-tecnologia, è riprodotto per grandi linee nel Resoconto riportato in *Teutas*, n. 1, gen. 2009, http://www.teutas.it (cfr. Recensioni).

[2] Cfr. D. PULITANÒ, *Diritto penale*, Torino, 3a ed., 2009, 187, nonché in senso analogo, anche per il rilievo che segue, R. FLOR, Phishing, identity theft *e* identity abuse*. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 900.

[3] Sono i rilievi enunciati, nell'ambito del Convegno cit., da N. IRTI, al quale si rinvia altresì per una più ampia trattazione della problematica: N. IRTI, E. SEVERINO, *Dialogo su diritto e tecnica*, Roma-Bari, 1a ed., 2001, 30 ss. e 19 s. Gli accenni che seguono trovano compiuta esposizione in N. IRTI, *Il salvagente della forma*, Bari, 2007, in part. 11 ss. e ID., *Nichilismo giuridico*, 2a ed., Bari, 2005, 34 ss.

[4] Cfr. altresì, anche per la notazione che segue in testo, N. IRTI, *S-confinatezza*, in *Studi in onore di Giorgio Marinucci*, a cura di E. Dolcini e C.E. Paliero, vol. III, Milano, 2006, 2925 ss. e dello stesso Autore l'intervento al Convegno cit.

[5] Interrogativi essenziali, per i quali si rinvia anche a FLOR, *loc. ult. cit.*

[6] Così, anche per i rilievi antecedenti, F. MUCCIARELLI, *Computer (disciplina giuridica del) nel diritto penale*, in *Dig. Disc. pen*., vol. II, Torino, 1988, 375 ss.

[7] Cfr. V. MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. ec*., 1992, 367; ritiene non condivisibile una differenza sostanziale tra la problematica emergente dall'elettronica applicata e quella "comune", nell'ambito del diritto penale G. MARINI, *Condotte di alterazione del reale aventi ad oggetto nastri ed altri supporti magnetici e diritto penale*, in *Riv. it. dir. proc. pen.*, 1986, 382.

[8] Per la consultazione si rinvia a V. MILITELLO, *Appendice* a *Nuove esigenze*, cit., 377 ss. A margine del fenomeno, ed in ragione della tutela di una «libertà informatica», G. PICA, *Reati informatici e telematici*, in *Dig. Disc. pen.*, *Agg.* I, Torino, 2000, 522 ss.

[9] Cfr. MILITELLO, *Nuove esigenze*, cit., 373 ss.

[10] Così F. MUCCIARELLI, *Commento* sub *art. 1*, *L. 23/12/1993 n. 547. Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, in *LP*, 1996, 57 s.

[11] In tal senso F. MANTOVANI, *Diritto penale*, *P. spec.*, I – *Delitti contro la persona*, 3a ed., Padova, 2008, 498 ss.

[12] In margine, L. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, n. 6/2008, 700 ss.; M. CUNIBERTI, G.B. GALLUS, F.P. MICOZZI, *I nuovi reati informatici*, Torino, 2009, in part., 7 ss.

[13] L'elaborazione risale anche alla giurisprudenza, Cass., Sez. VI, 4 ott. 1999, n. 3067, in *Cass. pen.*, 2000, 2990 ss. ed *ibid.*, S. ATERNO, *Sull'accesso abusivo a un sistema informatico o telematico*, e L. CUOMO, *La tutela penale del domicilio informatico*, 2998 ss. Per il precedente riferimento alla dottrina, circa l'oggettività giuridica della riservatezza, cfr. MANTOVANI, *Diritto penale*, cit., 518 ss. e *retro*, 500 s.

[14] Così G. MARINI, *Delitti contro la persona*, Torino, 2a ed., 1996, 367 s. e 385.

[15] Cfr. MANTOVANI, *Diritto penale*, cit., 518 e *ivi*, 529, per la notazione che segue.

[16] Così MANTOVANI, *Diritto penale*, cit., 529, ed altresì cfr. gli ulteriori rilievi, anche sotto il profilo costituzionale, *ivi*, 557 ss.

[17] L. PICOTTI, *Commento* sub *art. 3*, *L. 23/12/1993 n. 547*, cit., 69, ove si prospetta «un corrispondente *nuovo* interesse collettivo».

[18] Cfr. L. PICOTTI, *Commento* sub *art. 5*, *L. 23/12/1993 n. 547*, cit., in part. 110 s.

[19] II dato emerge dal documento «Una politica globale di lotta contro la criminalità informatica», in http://ec.europa.eu/italia /attualita/archivio/giustizia-liberta/112b44253fO_it.htm .

[20]
Così F. CAJANI, «Criminalità comune e uso degli strumenti informatici» (26 sett. 2007) – CSM, Incontro di studio sul tema: "Innovazioni tecnologiche e criminalità informatica", Roma 26-28 sett. 2007, 7. Il fenomeno complesso del *phishing*, nella sua qualificazione giuridica, è altresì affrontato in ordine alle sue implicazioni da F. CAJANI, *Profili penali del* phishing, in *Cass. pen.*, 2007, 2294 ss.; cfr. inoltre F. CAJANI, G. COSTABILE, G. MAZZARACO, Phishing *e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, 2008, in part., 112 ss.

In ordine all'interpretazione dell'art. 640 *ter* c.p. in ambito giurisprudenziale, Cass.pen., Sez. V, 24 nov. 2003, n. 4576, in http://www.penale.it/stampa.asp?idpag=115 .

[21]
Cfr. CAJANI, COSTABILE, MAZZARACO, Phishing, cit., 117, circa la configurabilità della fattispecie oggetto dell'art. 494 c.p.; ne evidenzia diversamente, con opportuni rilievi, i limiti FLOR, Phishing, cit., 907 ss. La «forma vincolata commissiva» prevista per il delitto, da cui consegue l'induzione in errore, esigerebbe evidentemente il riprodursi delle modalità normativamente determinate.

Per un'analisi puntuale della fattispecie in riferimento alle forme di realizzazione previste, A. PAGLIARO, *Falsità personale*, in *Enc. dir.*, vol. XVI, Milano, 1967, 646 ss.; V. MANZINI, *Trattato dir. pen. it*., 5a ed. (agg. da P. Nuvolone e G.D. Pisapia), vol. VI, Torino, 1983, 974 ss.; A. SANTORO, *Sostituzione di persona*, in *Enc. Forense*, vol. VII, Milano, 1962, 134 ss., nonché A. CRISTIANI, *Il delitto di falsità personale*, Padova, 1955, in part. 106 ss., ove si sottolinea che l'errore dovrà essere causato mediante «uno dei mezzi descritti dalla norma», così 113.

Si può altresì sottolineare – in margine alle modalità previste – il dibattito critico emerso, in sede di predisposizione del codice penale, soprattutto attraverso gli interventi della Magistratura. Si dubitava allora della collocazione della fattispecie tra i *delitti contro la fede pubblica*, a fronte di un ambito nel quale «il singolo è arbitro di accordare, o meno» fiducia; la stessa ove accordata rimarrebbe «*intuitu personae*, perché il fatto che una tale privata fede subisca un tradimento, non scuote la pubblica fiducia» - cfr. *Lav. prep. cod. pen. e cod. proc. pen.*, vol. III - *Osservazioni e proposte sul Progetto preliminare di un nuovo codice penale*, Parte III, Roma, 1928, 379 ss.

[22]
Cfr. Trib. di Milano, 10 maggio 2004, in *Giur. merito*, 2004, II, 2012 s.; in altro senso, fra le altre, per la configurabilità della «sostituzione di persona» a fronte della «situazione di affidamento nell'interlocutore telefonico», Cass., Sez. V, 11 dic. 2003, in *Cass. pen.*, 2005, 2993 ss., ed *ibid.*, R. CAPPITELLI, *La sostituzione di persona nel diritto penale italiano*. Per il richiamo, che segue nel testo, al progetto di modifica contenuto nel disegno di legge n. 1869/2009, lo stesso è reperibile sul sito del Senato della Repubblica, mentre per le ulteriori notazioni, di cui si dà conto, cfr. Associazione Bancaria italiana – Camera dei Deputati (Commissione Finanze), «Credito al consumo» - 10 nov. 2009 - Audizione del Direttore generale dell'ABI G. Sabatini, Audizioni ABI, 2009, ed *ibid*. «Appendice», circa le «frodi per furto d'identità». È ivi altresì enunciato il DDL n. 2699, in margine alle "Disposizioni di contrasto al furto d'identità e in materia di prevenzione delle frodi nel settore del credito al consumo, dei pagamenti dilazionati o differiti e nel settore assicurativo", a suo tempo approvato dal Senato.

[23]
Cfr., a margine dei rilievi esposti, CAJANI, COSTABILE, MAZZARACO, Phishing, cit., 117 s. ed *ibid*., nntt. 103 e 104. Collocata nell'ambito delle comunicazioni telematiche, la "posta elettronica", in quanto scambio di notizie, dati e messaggi, viene descritta quale forma di "corrispondenza", come del resto si evince dal «parere» su *e.mail* e *privacy* reso dal Garante e consultabile in http://www.repubblica.it/online/internet/lettere/testo/testo.html . Di recente, nell'ambito della giurisprudenza di legittimità, la sentenza della Cass. pen., Sez. I, 17 giugno 2010 ha sottolineato nello strumento della posta elettronica l'evidente «analogia con la tradizionale corrispondenza epistolare in forma cartacea». Complesso risulta tuttavia il rapporto tra informatica e normativa penale, in particolare in riferimento agli estremi di configurabilità del falso in scrittura privata *ex* artt. 485 e 491 *bis* c.p. Se non si fa a meno di annoverare tra i documenti firmati elettronicamente anche l'*e-mail*, vi è chi, pur riconoscendone la natura di «documento informatico», a fronte di una firma elettronica peraltro «"semplice o debole"», sottolinea come «la sua associazione al soggetto», dalla cui casella di posta elettronica risulti inviata, sia incerta e «piuttosto debole»: così, per tutti, C. CONSOLO, *Il processo di primo grado e le impugnazioni*, Tomo III, Padova 2009, 288 s., cui si rinvia anche per la nozione di *firma elettronica*.

Profili più strettamente penalistici sono esposti, a margine delle modifiche apportate all'art. 616 c.p. da L. PICOTTI, *Commento sub* art. 5, *L. 23/12/1993 n. 547*, cit., 109 ss.; cfr. altresì, R. RINALDI e L. PICOTTI, *Commento* sub *art. 6*, *ibid.*, 119 ss., nonché MANTOVANI, *Diritto penale*, cit., 502, per il quale la "posta elettronica" inerisce al «servizio di teletrasmissione di informazioni scritte dal mittente al ricevente».

[24]
Cfr. sul punto, e per il rilievo che segue, MARINI, *Delitti*, cit., 418 ss e 424 ss., il quale sottolinea l'occasionalità dell'intercettazione rispetto alle condotte di alterazione o soppressione. La qualificazione giuridica, *ex* art. 617 *sexies* c.p., è ammessa da S. FRATTALLONE, Phishing*, fenomenologia e profili penali: dalla nuova frode telematica al* cyber-*riciclaggio*, in http://www.globaltrust.it/documents/press/phishing/EnTrustAvv_Frattal-IonePhishing08Set05.pdf . La problematica è sottolineata da CAJANI, COSTABILE, MAZZARACO, Phishing, cit., 118, mentre la configurabilità è richiamata da R. GARGIULO, sub *art. 617*-sexies, in G. LATTANZI, E. LUPO (dir. da), *Codice penale – Rassegna di giurisprudenza e di dottrina*, vol. V, Milano, 2005, 669 s. Dal punto di vista operativo, si può segnalare come il Compartimento Polizia Postale e delle Comunicazioni per la Lombardia (Milano) assuma la configurabilità dell'art. 617 *sexies* c.p. in caso di falsa formazione del contenuto di *e-mail*, simulandone la provenienza da parte di Istituti di credito reali. Va rilevato come nella dottrina PICOTTI, *Commento* sub *art. 6*, cit., pur sottolineando la problematicità del concetto di "comunicazione", a fronte della «ridondanza di previsioni sanzionatorie» e «interferenze applicative», escluda che «nel caso di "formazione" del falso *ex novo*» possa l'intercettazione, proprio per la tipologia della condotta, esplicare «alcun ruolo condizionante» - così 124. Si rileva peraltro il complesso intreccio di norme introdotte: si pensi al dettato dell'art. 617 *ter* e all'art. 623 *bis* c.p., per cui si giunge a prospettare al contempo una «*duplicazione*» e la conseguente problematicità rispetto ad un possibile «confine reciproco» tra norme vigenti - 122 ss., *ibid.*, nt. 17 e *retro* – sub *art. 5* – 111 ss. Diverse le conclusioni interpretative svolte da R. FLOR, *Frodi identitarie e diritto penale*, in http://www.penale.it/stampa.asp?idpag=730, cui si rinvia anche per la pronuncia del G.I.P. di Milano, sent. 10 dic. 2007, n. 888, che nel caso di specie ha ravvisato la configurabilità dell'art. 617 *sexies* c.p.

[25]
Così MANTOVANI, *Diritto penale*, cit., 561 e *ibid.*, in conseguenza dei rilievi che precedono, la proposta, a fronte della normativa vigente, dell'eliminazione della «complicatoria distinzione tra corrispondenza e comunicazione». Circa la condotta della fattispecie in esame, cfr. altresì, *ivi*, 588 s., da cui emerge che anche l'occasionale intercettazione è ricondotta alle sole ipotesi di *alterazione* e *soppressione*. Cfr. in altro senso PICOTTI, *Commento*, sub *art. 6*, cit., 124, ove l'Autore, nel rilevare quale nuovo oggetto di tutela «le stesse condizioni di sicurezza ed affidabilità dei sistemi informatici e telematici da manipolazioni illegittime», solleva al contempo perplessità circa la gravità della sanzione a fronte di una fattispecie dai confini incerti.

[26]
Cfr. G. MARINI, *Delitti contro il patrimonio*, Torino, 1999, 409; ID., *Truffa*, in *Dig.Disc. pen.*, Torino, 1999, 353 ss., dove l'A. si sofferma a sottolineare «la derivazione causale del danno e del profitto ingiusto dal comportamento patrimonialmente rilevante del titolare del "potere di disposizione"», ovvero destinatario della condotta, così 374 ss. Analogamente, *ibid*.- cfr. altresì nt. 136 -, puntualizzato il verificarsi del danno e profitto ingiusto tramite il cosiddetto atto di disposizione, si ribadisce la questione inerente al «comportamento dispositivo dell'ingannato», per approfondirne i profili psicologici - 377 ss. Dello stesso A., in precedenza, *Profili della truffa nell'ordinamento penale italiano*, Milano, 1970, in part. 163 ss. L'elemento della cooperazione della vittima, riletto «come apporto consapevole», viene sottolineato da R. ZANNOTTI, *La truffa*, Milano, 1993, in part. 80 ss.; lo stesso elemento viene confrontato nei contenuti con la «soluzione più corretta», che nella interpretazione dottrinale del Pedrazzi «richiede una volontà consapevole del soggetto passivo», con l'effetto di *indurlo* a «compiere un'azione patrimonialmente dannosa» - cfr. altresì, ivi, l'autorevole dottrina cit. Di recente, a margine del *requisito tacito* o *implicito* della truffa, A. FANELLI, *La truffa*, 2a ed., Milano, 2009, 49 ss. Significativa, inoltre, la notazione di I. CARACCIOLI, *Reati di*

mendacio e valutazioni, Milano, 1962, 138, in merito alla truffa, quale delitto «che attenta alla libertà del consenso nei negozi patrimoniali».

[27] Così MANTOVANI, *Diritto penale*, cit., 530 e 581. Per i riferimenti normativi, che in testo precedono, si rinvia alla dottrina più volte citata per gli opportuni rilievi di natura sistematica.

[28] MARINI, *Delitti contro il patrimonio*, cit., 458 s., a margine dell'art. 12, D. l. 3 maggio 1991 n. 143, conv., con modif., dalla L. 5 luglio 1991 n. 197. Per il testo della pronuncia dianzi cit. si rinvia a FLOR, *Frodi identitarie*, cit., ed *ibid*., nt. 1.

[29] Cfr. MANTOVANI, *Diritto penale*, cit., 563.

[30] Cfr. in tal senso i rilievi svolti da V. ZENO-ZENCOVICH, *Repressione della criminalità informatica e tutela dei diritti fondamentali*, in *Diritto @ Storia* 7, 2008 = http://www.dirittoestoria.it/7/D-&-Innovazione/Zeno-Zencovich-Criminalit-informatica-tutela-diritti.htm, il quale prospetta altresì la necessità di «costruire la norma attorno all'esigenza di tutelare la identità digitale del soggetto, espressione della sua persona».

[31] Progetto in *La riforma del codice penale*, Schema di delega legislativa per l'emanazione di un nuovo codice penale, in *Doc. giustizia*, n. 3/1992, in part. 372 ss. e 423 ss. Nello stesso Progetto si è prevista altresì, nell'ambito dei *reati contro la riservatezza delle comunicazioni*, la fattispecie, oggetto dell'art. 76 – 6), del seguente tenore: *accesso abusivo ai sistemi informatici, consistente nel prendere cognizione di dati di un sistema informatico di elaborazione, contro la volontà espressa o tacita di chi ha il diritto di escluderla, sempre che il fatto non costituisca un più grave reato.*

[32] Cfr. E. ANCONA, *Figure dell'ordinamento. Dalla piramide alla rete, e oltre...*, in http://www.filosofiadeldiritto.it/1%20Dottrina%202007.1.htm e più in generale, circa una possibile «*configurazione reticolare* del diritto», P. HERITIER, *Urbe-internet*, vol. 1 - *La rete figurale del diritto*, Torino, 2003, 44 ss.